This sample chapter is for review purposes only. Copyright © The Goodheart-Willcox Co., Inc. All rights reserved.

15 PC Troubleshooting

After studying this chapter, you will be able to:

- ✔ State commonly practiced troubleshooting steps.
- ✔ Identify the three stages of computer operation.
- ✔ Recognize common startup problems and understand their causes.
- ✔ Restart a PC in a variety of troubleshooting modes.
- ✔ Identify the appropriate diagnostics utility to use given a specific problem.
- ✔ Step through a PC's boot sequence.
- ✔ Explain basic data recovery methods.

A+ Exam—Key Points

A+

The A+ Certification exams place a great deal of weight on knowing the basics of troubleshooting. You need to become familiar with the tools, their limitations and their purpose. The best way to become familiar with troubleshooting tools is by using them. Study the menu options, such as **Safe Mode**, and how to access them.

It is very important to study the setup readme.txt files that come with each version of Windows installation CDs. They contain a lot of information that is used on the A+ Certification exams and that is usually not found in textbook material.

Key Words and Terms

The following words and terms will become important pieces of your computer vocabulary. Be sure you can define them.

- blue screen error
- clean room
- differential backup
- incremental backup
- kernel mode
- Microsoft Dynamic Link Library (DLL)
- startup problem
- user mode

Troubleshooting a PC requires a combination of the technician's knowledge, intuition, and experience. There are many diagnostic tools that are included as standard programs for Microsoft software systems. There are also many diagnostic tools available from third-party vendors that can assist in the troubleshooting process. Third-party vendor programs range from freeware and

shareware to systems costing several thousands of dollars. The more expensive programs include a diagnostic board that plug into the PC's expansion slots.

Most problems can be diagnosed without expensive system diagnostics. The value of expensive diagnostic tools is they can be used to save time and money when trying to identify problems that may be caused by two or more components. For example, it can be difficult to determine if a problem is caused by a troublesome CPU or a bad motherboard. When this situation arises, a simple solution is to substitute a known or good CPU for the suspect CPU. However, this substitution alone can be a very expensive proposition.

Common Sense Practices

Remember, when troubleshooting and repairing PCs that "time is money." When diagnosing PC failures and problems, always take the quickest and easiest path first. When troubleshooting, there are some common sense practices you should follow:

- ✔ Determine the major area at fault.
- ✔ Determine what action occurred just prior to failure or problem.
- ✔ Write down settings before you change them.
- ✔ Go slowly.
- ✔ Think, think, think!

Determining the Major Fault Area

The first step is to try to determine what major area is the most likely source of the fault. There are three major fault areas to be considered:

- ✔ Hardware failure.
- ✔ Software failure.
- ✔ User-generated problems.

The most common error or problem is the user-generated problem. Some users like to tinker with Control Panel, and others will try to solve their problems alone. Users with a little technical knowledge can be the most dangerous. They often attempt to fix a problem alone before calling the technician. When this happens, you may very well be faced with more than one problem. First, the original problem likely still exists, and then there are additional problems created by the user. Repairing computers in a school setting can be the most frustrating. Some students love to experiment on the settings on a school's computer before trying the activity on their home computer.

What Happened Last?

It is critical to determine from the computer user what the last action on the computer was prior to the problem occurring or before computer failure. Often, the last action taken by the user can lead the technician directly to the problem. Find out if the user recently installed some new software. Perhaps, there has been a recent hardware upgrade to the problem PC. Has the user recently downloaded a file from the Internet? Ask as many questions of the user as possible. This can save valuable time.

Proceed Carefully

Do not rush when diagnosing problems. Operating in a hurry will lead to sloppy work. This can create new problems or cause you to overlook something important. In contrast, do proceed in a methodical yet constant pace. Customers will not appreciate a technician who is standing around drinking coffee, talking, socializing, or any other activity that appears to be a nonproductive use of energy. Customers are typically paying a premium price for service and are losing the use of their computers while they are inoperable. Don't waste their money, or, next time there is a problem, someone else will be called.

Write Things Down

Do not rely on your memory alone while performing troubleshooting. Before you change a setting, write down the current setting. If you are going to delete a file, write down the file name. You can make the problem much harder to find if you create another problem along the way. If a problem is not cleared after changing a setting or deleting a file, you should return the system file or setting to the way you found it. Do not simply move on and try something else.

Think

Think the problem through. Don't try operations out of desperation. Desperate technicians will often run the same test twice knowing the results from the first test were valid. These are acts of desperation, and they occur when a technician is stumped.

When you run out of tests—*stop and think* about the situation. Writing things down in a list helps. Make two lists. First, make a list of what you know is not the problem. Then, make a list of possible problems that could still exist. Check the Web site of the manufacturer of the PC, the BIOS, and the operating system. There could be corrections posted for exact symptoms you are encountering. Many times, a problem is discovered that affects a particular setup or particular combination of hardware and software programs.

Don't hesitate to contact the manufacturer of the hardware or software in question by e-mail with a description of the problem. Most questions will be answered in 24 to 48 hours at no cost for the service. You can get much faster replies by calling, but that service is seldom free.

Your fellow technicians are another very important source of information. As you progress in the PC repair world, you will make many friends. It is a standard practice to share information with a colleague who may have encountered a similar problem. A peer may have a quick and easy answer to a problem that you have not encountered before. Other times, simply discussing the problem with a peer can be quite helpful. Explaining the problem forces you to summarize the situation and describe it in logical terms. Just the act of verbalizing the problem may allow you to solve it. Never be embarrassed to use this form of assistance.

Troubleshooting Overview

There is no one foolproof method to troubleshooting. There are too many variables that can cause a computer to fail, but there are recommended procedures that can be used to help you organize your approach to solving a computer problem. The causes of failure discussed are not all inclusive and should be interpreted as a guide to solving a computer-related problem or complete system failure.

When troubleshooting computer problems, the first thing you must do is isolate the problem. You must determine if it is a hardware problem, software problem, or user-generated problem. This is easier said than done. The best way to go about this is to decide when the problem is occurring. In other words, at what stage of computer operation is the problem occurring? Did the failure or problem happen during the POST, during the loading and initialization of the required operating system files, or after the logon and running the services and application software? This section discusses the common causes of failure related to the three stages of computer operation. The first stage is the POST. The second stage is loading the required operating system files and initializing the hardware system. The third stage is after the logon. It comprises loading the startup programs and running applications and services.

First Stage

If the problem occurs during POST, it is most likely a hardware failure. In this stage, no operating system software or allocation software has been loaded. The post may fail to complete if a damaged hardware device fails POST or fails its own diagnostic routine. For example, a telephone modem that has been damaged during a thunderstorm may cause the computer to lock up during the POST or immediately after.

If you just built the computer system and it fails to successfully boot the first time during POST, chances are you have improperly installed the RAM, CPU, or CPU cooling device. A high-speed CPU that has an improperly installed cooling fan and heat sink may generate excessive heat in a few seconds, causing the computer to freeze while performing the POST. Improperly seated RAM may also cause the computer to fail during POST. When memory is improperly seated, a beep code typically will be issued, indicating a problem with RAM. Go back and reinstall these devices and remove all unnecessary devices, such as adapter cards that are not required for system operation, and reboot the system.

If the problem still persists, you can either substitute parts to determine which hardware device is causing the failure during POST or use a third-party utility that uses a POST card to diagnose the POST problem. A very popular third-party utility suite used by repair centers is PC-Doctor Service Center 6. The complete PC-Doctor Service 6 kit is shown in **Figure 15-1.**

The kit includes all the software and hardware you need to perform a thorough testing of all computer hardware components. PC-Doctor is used by Circuit City firedog technicians as well as Staples to perform computer diagnostics in the service department.

The PC-Doctor POST card, **Figure 15-2,** is inserted into any PCI slot and used to diagnose errors during POST caused by hardware failure such as the CPU, RAM, or the motherboard. A POST error code is displayed on the LEDs. The technician can then match the code to the diagnostic chart in the user manual.

Figure 15-1. The PC-Doctor Service Center 6 is a complete kit for diagnosing computer hardware. (PC-Doctor, Inc.)

Figure 15-2. PC-Doctor PCI POST card. (PC-Doctor, Inc.)

Without a POST card, a technician would have to substitute the CPU, RAM, and motherboard with a known good component. Part substitution can be very time-consuming and expensive. The technician runs the risk of damaging a part during the substitution process.

For more information on problems that can occur during the POST stage, see the following chapter sections: Typical Startup Problems, Hard Drive Failures, Additional Mechanical Problems, and Boot Sequences.

Second Stage

If the problem occurs during stage two—operating system loading and initialization—the problem is most likely related to a corrupt operating system file or a driver. You can identify when stage two starts by observing the screen display. Many computer systems display the results of the POST as it occurs. You will see the RAM check verified on the screen as well as the hard disk drive identified and other devices present. Soon after the POST turns over loading the

operating system to the boot strap program, you will see a progress bar appear on the screen. When you see the progress bar, you know that the second stage has begun and the operating system has successfully loaded the system kernel. The operating system then initializes the hardware devices.

Failure during the second stage is usually the result of a corrupt required operating system file such as ntldr or failure to properly detect and initialize a piece of hardware such as the sound card. It can also be the failure of a required hardware driver file.

The fastest way to repair a system failure that occurs during the loading and initialization of the operating system is by reinstalling required system files. Simply insert the installation CD/DVD and then reboot the computer. When the installation CD/DVD boots, follow the screen prompts. For more information on problems caused by hard drive failure that can occur during the second stage, see the Hard Drive Failures section. Detailed troubleshooting methods for this stage are covered in the Recovering from a System Startup Failure section.

Third Stage

System logon is the end of the second stage. Keep in mind that not all operating systems require a logon. The third stage is when the desktop first appears. During the third stage, startup programs, services, and applications are loaded. The most common problems that can occur during this time are usually due to corrupt or incompatible drivers and files.

File corruption

Files can become corrupt in various ways such as by virus attacks and hardware failures. For example, an intermittent RAM failure can corrupt files also if the file contents is being transferred or copied during the time of RAM failure. Files are also corrupted by being stored in an area of the hard drive that has a bad sector. All data saved to the bad sector is lost, thus corrupting the contents of the complete file.

Overwritten DLL file

Microsoft Dynamic Link Library (DLL) an executable file that can be called and run by Microsoft software applications or by third-party software programs.

Certain files such as DLL can cause a system failure when inappropriately applied in a software program or when they become corrupt. A ***Microsoft Dynamic Link Library (DLL)*** file is an executable file that can be called and run by Microsoft software applications or by third-party software programs. Rather than write code from scratch each time a new software application is written, a programmer can simply call a DLL from within the program they have written and run the function they need automatically. One DLL can be used by more than one software program at the same time. By reusing the same code contained in the DLL, a programmer saves time and the computer uses less memory and disk space. The term *dynamic* is used because the file can be loaded, run, and then unloaded from computer memory when no longer needed.

One of the major software problems in the past is when a user loads a software application from a disc that contains the necessary DLL files required to run their software application. All too often, the DLL file on the software disc overwrites the existing DLL already residing on the computer. If an older DLL file overwrites a newer DLL file, an error can occur when the user starts an application other than the one just loaded. A classic example is when a user loads an older version of a software game on a computer that has other games

requiring the similar DLL file. While the older game runs perfectly, one or more of the other games may now run incorrectly or may not run at all.

DLL files usually have a DLL file extension such as mon.dll. Sometimes the DLL will have an .exe file extension. Look at **Figure 15-3** to see the results of a search for files with the "dll" extension. There are 11,497 files that have a "dll" extension on this particular computer. As you can see, there are thousands of possible DLL files that can be used as part of software application programs and hardware drivers.

Blue screen error

The system may also experience a blue screen error. A ***blue screen error*** is a blue screen that appears with an error code and then freezes the system. Microsoft also refers to blue screen errors as *fatal errors*, *stop errors*, and *stop error messages* because the system is not recoverable at the time of the error. The system must be restarted before you can attempt to remedy the problem. Some of the most common causes for blue screen errors include the following:

blue screen error a blue screen that appears with an error code and then freezes the system. Also referred to by Microsoft as fatal errors, stop errors, and stop error messages.

- ✔ Defective hardware, such as memory chips and video adapter cards.
- ✔ Corrupt files on the hard drive.
- ✔ System BIOS settings that are beyond the capabilities of the hardware.
- ✔ Third-party software containing bad code.
- ✔ Bad code in the Windows operating system.

The error codes displayed on the blue screen can be quite cryptic. You should copy the error code and use it as a reference when searching Microsoft's support Web site.

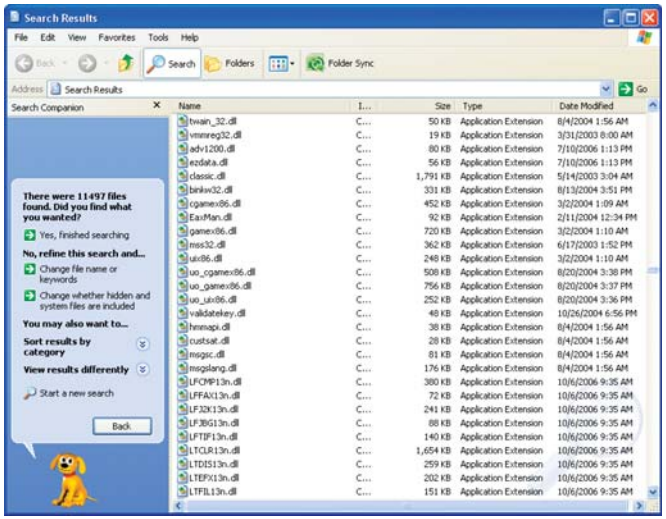

Search Results
File Edit View Favorites Tools Help
Search Folders Folder Sync
Address Search Results
Search Companion
There were 11497 files found. Did you find what you wanted?
Yes, finished searching
No, refine this search and...
Change file name or keywords
Change whether hidden and system files are included
You may also want to...
Sort results by category
View results differently
Start a new search
Back
Name Size Type Date Modified

Figure 15-3. DLL files are called by software applications to perform common tasks.

The most appropriate utility for diagnosing a problem after the logon is the System Configuration Utility (msconfig.exe). This and other utilities for diagnosing problems during this stage are covered in the Recovering from a System Startup Failure and the Windows Diagnostic Utilities section.

A malicious software program (virus or worm) can attack a computer at any time, not just after the system logon. For example, if the MBR is corrupted by a virus, the computer will fail before switching from text mode to graphic mode.

Typical Startup Problems

startup problem problem that causes the computer to lock up during the boot process.

Startup problems are a tough class of computer error that you are bound to run into. A ***startup problem*** is a problem that causes the computer to lock up during the boot process. These problems occur too early in the PC operation to be solved by system diagnostic tools. This section details some of the most common and catastrophic boot problems that you will encounter while starting the PC. Each of the following problems is described as a symptom. Possible solutions are provided as a guide. The list of symptoms is condensed and centers on the problems encountered before the boot process is completed. Keep in mind that there are hundreds of possible computer symptoms. What follows are a few of the most common system hardware failures during the boot.

Think about the boot process and the steps involved. System boot failures involve the power supply, CPU, hard drive (boot device), BIOS, CMOS, system configuration, autoexec.bat file, loading of drivers, and the loading of the operating system. Now let's look at some of the most common hardware problems and their symptoms during the boot process.

When reading the list that follows, assume that there is one hard drive labeled C and a CD drive labeled D. Note that these are recommended procedures, not absolute procedures. Also, viruses can imitate some of the described symptoms. Always check for the presence of a virus and protect your disk while doing so.

Remember, always attempt the simplest tests first. Then, move on to the more complex and labor-intensive tests.

Symptom 1:

There is no power light, no fan running, and no sound of boot operation at all. It appears that the PC is completely dead.

Items to check:

Before you open the case, make sure the PC is plugged in. Next, check the power from the wall outlet or power strip or both. Be sure there is power to the unit. If you have power, then the likely problem is the computer's power supply. Open the case and test the power supply outputs. Swapping out power supplies is generally more cost effective than fixing a broken one.

Symptom 2:

The power light (LED) is on and the fan is running, but there is no activity. The system appears dead.

Items to check:

Check the power supply for a power good signal. The *power good signal* is sent back to the BIOS system to signal that the power supply is on and ready. The signal back should be approximately 5 volts. Pin 1 is usually the power good pin. Pull the connector back just far enough to check for 5 volts (+/–1 volt). If the power is very low, there may not be sufficient voltage to power up the system. The power output does not have to be completely dead to affect startup.

If the power good signal checks out, check the connection from the power supply to the motherboard. Reseat this connection. Try reseating the CPU. Sometimes the CPU is not making a good electrical contact. CPUs operate on fairly low voltages. A slight oxidation buildup on one of the CPU's pins that is operating at 3.3 volts is sufficient to render the CPU dead. Cleaning the oxidation will bring it back.

If you perform all of the listed operations and the system still fails to activate, you *probably* have a defective motherboard.

Symptom 3:

The system tries to boot. There are two or more beeps, and then nothing (no video). The fan is running, and there is a power light.

Items to check:

Make sure the monitor is plugged in correctly (both the data plug and the power cord). Check the video card. Try reseating the card. If those actions do not help, try to decode the beep error code. If you have the manual that came with the motherboard, start there. Newer manuals are often CDs as opposed to the traditional paper booklet. If there is no manual, look up the BIOS chip manufacturer on the Internet. First, copy all information from the BIOS chip or motherboard and then head to the manufacturer's Web site.

Symptom 4:

You see a setup error indicated on the screen.

Items to check:

This is probably a CMOS setup problem. Access the BIOS setup routine by using the key combination indicated on the screen. If no setup routine is given, try key combinations you are familiar with. Some popular combinations can be found in Figure 3-39 from Chapter 3—Motherboards. You can also look up the keystroke combination for accessing the BIOS at the BIOS manufacturer's Web site.

Normally, CMOS settings do not change. However, sometimes when you install a new hard drive and the drive is automatically detected, the settings change. Also, if the battery used to hold the CMOS data is going bad, you could lose the settings. The date and time not matching the true date and time is a good indication that your battery is going bad.

Be sure to write down the existing CMOS settings before you make any changes to them. This is extremely important if you are going to try something like the **Return to default settings** option. When that option is selected, many settings will change instantly, and you will not be able to tell which settings have changed or what they changed from. Check the manufacturer's Web site for the correct CMOS settings for your particular model of PC.

Sometimes people get curious and go into the BIOS setup to see what it looks like. They also make changes either intentionally or accidentally. What makes it worse is they generally deny going into the setup program.

Symptom 5:

The PC powers on, but there is no drive activity.

Items to check:

Check the system CMOS settings. Make sure the drive is identified. The drive should be identified in the setup program as far as the number of cylinders, heads, and sectors. In addition, while the PC is booting, the hard drive manufacturer followed by the hard drive model number will often flash on the screen when the BIOS finds it. If the drive is not detected during the boot, the screen will flash something similar to "No Hard Disk Drive."

You should also check the connections between the power supply and the hard drive and the motherboard and the hard drive. They should be tight.

If all that checks out, boot the system with a boot disk. From the command prompt, see if you can access the hard drive. If you can access the hard drive, change your default directory to C:\Windows. When in the Windows directory, type **win** to see if you can start Windows.

Symptom 6:

There is normal boot activity, lights and sounds, but no video.

Items to check:

Check if the monitor is plugged into the computer and that the monitor has power. Swap the monitor out for a monitor that is known to be good. If the system still fails to generate a display, you probably have a bad video adapter card. Try reseating the video adapter card. If the system will still not display, change the video adapter card.

Symptom 7:

The system crashes or reboots for no apparent reason.

Items to check:

Check the power supply and cables. Make sure they are all tight. Check for excessive heat on the CPU and memory chips. Make sure all DIMMs are seated properly. Try reseating the CPU.

If all of that hardware checks out, you likely have a defective motherboard or there is a problem with the hard drive. Swapping hard drives with one you know is working should show you where the problem lies. If the hard drive is causing the problem, check for a virus or a corrupt operating system. Always think about the last thing that occurred on the PC before the problem developed. For example, did you or your client recently install a new software program? The following section looks at hard drive failures in more detail.

Hard Drive Failures

Hard drives fail more often than would be thought. Any component that is an electronic and a mechanical combination will fail after a period of time. In addition, hard drives can fail because of software issues. A corrupt MBR can cause hard drives to be unresponsive. It is important for you to determine more than just if a hard drive is bad. You must also determine why it is bad.

A bad hard drive or a corrupt MBR will generate a screen message such as one of the following:

- ✔ Invalid partition table.
- ✔ Error loading operating system.
- ✔ Missing operating system.

If any of these three error messages appear, you most likely have a hard drive problem. To check, try booting the system from a floppy disk. If the system boots normally from the floppy, this will verify a hard drive problem.

Mechanical Hard Drive Failure

Mechanical parts wear out. A sure sign of an upcoming mechanical hard drive failure is an unusual sound coming from inside the computer when it is being accessed (a read or write operation is being done). The sound may be a high-pitched whining sound or a clanking sound. The strange sound coming from the hard drive is mechanical in origin and cannot be repaired. Swapping out the bad hard drive is the only solution.

The only guaranteed method of fully recovering from a hard drive failure is by doing regular backups of the data. You can always reinstall a collection of software when replacing a hard drive, but the data will be lost unless a recent backup has been made. Users should be instructed to back up data regularly, but it is even more important when a hard drive makes strange sounds. Data should be backed up immediately, and a technician should be called to prepare for the crash. You should have parts on hand and be prepared to replace the hard drive.

MBR Failure/Recovery

Hard drives can also fail because of corrupted files and data. The most important area of the hard disk is the master boot record (MBR). If the MBR is damaged, the hard drive will not support the booting process. However, you will still be able to boot from a bootable floppy or CD. Once you boot from the floppy or CD, try to look at the hard drive by entering the **dir C:** command at the command prompt, **Figure 15-4.** If you can view the files on the hard drive, then you are in a position to do a repair. You probably will be able to remedy the situation. As a precaution, back up all data immediately.

You will not be able to back up the files in every situation. But, if you can see files on the hard drive, you should be able to back up important data to some kind of data storage media. Generally on an older system, you will be forced to do a copy to disk. Though, on some newer systems, you may be able to access the drive via an existing network connection. A modern computer with a bootable CD-RW allows for a quicker and easier backup of system files. You can boot the PC using a system restore CD. The CD is placed in the drive and loads all necessary files to boot the PC. In addition, you may load a driver to support the CD-RW. After the drivers are loaded for the CD-RW, you can copy files that need to be backed up.

Avoid using the **fdisk/mbr** command unless it is as a last resort. The **fdisk/mbr** rewrites the boot code portion of the MBR. The last two bytes in the MBR contain partition and volume information. If the last two bytes in the MBR were deleted by a virus, all partition information will be lost when you use the **fdisk/mbr**. Two situations are made worse by this command. One situation is when you have a multiple boot system using at least two partitions. The **fdisk/mbr** command can make the second partition inaccessible as well. It overwrites the partition table,

Figure 15-4.
Examine your hard drive through the command prompt. If you can see your files, you should be able to repair the drive and save the data.

MS-DOS Prompt
AD15F4AE MFD 587 08-22-01 11:47a AD15F4AE.MFD
MODEMDET TXT 64 09-12-01 3:36p MODEMDET.TXT
HPBAFD INI 331 12-13-01 8:43a hpbafd.ini
DIALER INI 512 08-29-01 10:07a dialer.ini
CALLLOG TXT 0 08-29-01 10:06a calllog.txt
DIRECTCC EXE 69,632 04-23-99 10:22p DIRECTCC.EXE
SFCLOG TXT 5,975 09-27-01 2:37p SFCLOG.TXT
HELPDESK <DIR> 09-27-01 3:08p helpdesk
IE4ERR~1 TXT 975 11-14-01 3:26p IE4 Error Log.txt
WINNT32 LOG 47 12-04-01 10:46a WINNT32.LOG
SETUP <DIR> 11-12-01 9:11a setup
SETUPACT LOG 90 12-04-01 10:46a setupact.log
SETUPERR LOG 0 11-12-01 9:11a setuperr.log
WPXINDEX LST 51 11-19-01 11:14a WPXINDEX.LST
PPDINDEX LST 166 11-19-01 11:14a PPDINDEX.LST
FONTS MFD 11,742 11-19-01 11:14a FONTS.MFD
APTOLLW1 WPX 11,085 11-19-01 11:14a APTOLLW1.WPX
WININIT BAK 138 11-20-01 11:28a WININIT.BAK
PARALL~1 LOG 1,337 12-05-01 3:32p Parallel cable or
290 file(s) 122,081,313 bytes
39 dir(s) 10,158.52 MB free
C:\WINDOWS>

the boot sector, and the file allocation table. This essentially erases any record of the other partitions. The second situation affects some older computer BIOS systems that cannot access large disk drives. A third-party tool called an *overlay program* is used to remedy the large disk access problem. The **fdisk/mbr** command can overwrite the information used by the overlay program to allow large disk support. This can further complicate or compound the program.

Many third-party software systems can repair an MBR, especially if the software is installed before the problem develops. The software recovery systems make a copy of all vital information including creating a copy of the MBR. When an error occurs, the recovery software can use the copy to help recover the damaged system. In addition, third-party software systems can be used to inspect, copy, and modify bytes in each sector of the hard drive. This is a very powerful tool, but using it can be very time-consuming.

Additional Mechanical Problems

There are a number of other mechanical faults that cause problems in PCs. Boards, cards, and cables can go bad, but these occurrences are not all that common. You will find that, along with hard drive failure, most of your other mechanical problems will arise from two areas: improper hardware upgrades and accumulation of dust in the system.

Problems after Hardware Upgrades

There are many possible system failures after a hardware upgrade. The first thing to check when a system fails to boot is the power and cable connections. Many times while working inside the case, cables are pulled loose. So, the first thing to look for is free-hanging cables. However, cable problems will not always be cables that were not reconnected. Sometimes when a cable is pulled loose, the user will inadvertently replace the cable incorrectly. The cable may be off one pin, or a pin may be damaged. Data cables can also be pinched when systems are reassembled.

Another major problem occurs when mixing different generation technologies together inside the same PC. When a PC has been upgraded several times, problems do arise. An older BIOS chip may not be able to recognize certain new memory module or see the vast new hard drive that has been installed. Check the system resources for conflicts. (Use the **System Properties** dialog box or the **Microsoft System Information** utility.)

Dust Accumulation

The accumulation of dust inside a PC is typical. The type of environment in which the PC operates, as well as its age, determines how much dust has accumulated. Large amounts of dust can cause heating problems by blocking air filters and by collecting on processor heat-sink fins and fan components preventing the proper dissipation of heat. The dust acts like an insulator and holds the heat to the CPU rather than allowing the cooling fins to dissipate it. The dust can clog air filters and render a fan inoperable.

Remove dust carefully using a can of compressed air or a special vacuum cleaner designed for PC cleaning. Standard vacuum cleaners can generate a tremendous amount of static electricity, which is very dangerous to computer chips. Use only vacuum cleaners made specifically for electronic equipment.

Removing dust from a CRT can be dangerous. Do not attempt to open and remove dust from inside a CRT without special training. There are dangerous voltage levels inside a CRT case that remain even after the CRT has been disconnected from electrical power.

Recovering from System Startup Failure

Recovering from a system startup failure requires the technician to have advanced skills. Many of the utilities described in this section should not be used by the inexperienced user because they can cause additional problems if not used correctly. To become an experienced technician, you should practice using these utilities in the lab before attempting to use them on a customer's PC. You can also download extensive information about each of the utilities from the Microsoft Support Web site.

Boot Options

There are a number of different modes you can boot your computer into other than the normal mode that your PC boots into by default. The other modes are used for troubleshooting the computer. You can force your computer to boot into these other modes. They are useful if your computer has any of the following symptoms:

- ✔ System stalls for an unusually long period of time.
- ✔ Printer problems (as a last resort only).
- ✔ Video display problems.
- ✔ Computer shuts down or locks up for no apparent reason.
- ✔ Intermittent error conditions.

Pressing the [F8] key during the boot process halts the boot process and displays a menu on the screen. These choices vary somewhat depending on the operating system you are using. A typical Windows 98 operating system lists the following options:

- ✔ **Normal**.
- ✔ **Logged**.
- ✔ **Safe Mode**.
- ✔ **Safe Mode with Network Support**.
- ✔ **Step-by-Step Confirmation**.
- ✔ **Command Prompt Only**.
- ✔ **Safe Mode Command Prompt Only**.
- ✔ **Previous Version of MS-DOS**.

Normal means that you start the PC as you normally would. The second choice, **Logged**, means that a log of boot activities will be recorded in a file called bootlog.txt stored in the root directory of drive C. The log contains information about which files loaded correctly.

Safe Mode will start automatically if Windows detects a system startup failure. In safe mode, Windows uses a basic configuration. Safe mode bypasses startup files such as config.sys, autoexec.bat, the registry, high memory, and parts of the system.ini. You will likely use this very handy option on a frequent basis. In this option, only the essentials are used to start the system giving you a chance to diagnose the computer. Safe mode disables Windows device drivers and starts the display in standard VGA mode. When in safe mode, each corner of the monitor screen displays the words "Safe Mode." You can force a Windows 98 or Me system to start in safe mode by holding down the left [Ctrl] key while booting.

Step-by-Step Confirmation operates as implied. It allows you the option to carry out or reject boot process files displayed on the screen on a step-by-step basis. This allows you to disable specific drivers called for in each line in the autoexec.bat and config.sys. By disabling each line, one at a time, you can determine which files and drivers are corrupt.

Command Prompt Only allows the computer to boot to the command line interface, not to the Windows graphical user interface. The command interpreter is loaded. A command prompt appears on the screen, and you are free to issue commands from the prompt such as **scandisk**, **dir**, and **copy**. You can start Windows from the command line simply by typing **win** and then pressing [Enter].

Safe Mode Command Prompt Only starts the computer with only the essential drivers as if in safe mode. It does not load the graphical user interface. The command interpreter is loaded and the command prompt appears allowing commands to be issued.

Depending on the version of Windows you are using, not all options will be available. For example, the **Last known good configuration** option is available from safe mode of Windows 2000, XP and Vista, but not in Windows 98 or Me.

Last known good configuration, when selected, uses the last set of registry data before the system failed. This selection assumes that a change occurred in the configuration of the computer system, which resulted in the system failure.

Windows Vista uses the [F8] function key to launch the **Advance Boot Options** menu. This menu is slightly different in appearance when compared to the menu of previous versions. **Figure 15-5** shows the **Advanced Boot Options** menu.

System Restore

System Restore can be used to restore a system to a previous working state. System Restore first became available in Windows Me. Restore points, which are backups of system settings and configurations, make it possible for a computer to revert to an earlier time when the computer system was working properly.

Look at **Figure 15-6.** When System Restore first opens, it provides two options: **Create a restore point** and **Restore my computer to an earlier time**. Although System Restore automatically creates restore points daily and before a software program is installed, the **Create a restore point** option allows the user to make a backup of the existing system. Creating a restore point manually should always be performed before changing configurations, adding hardware,

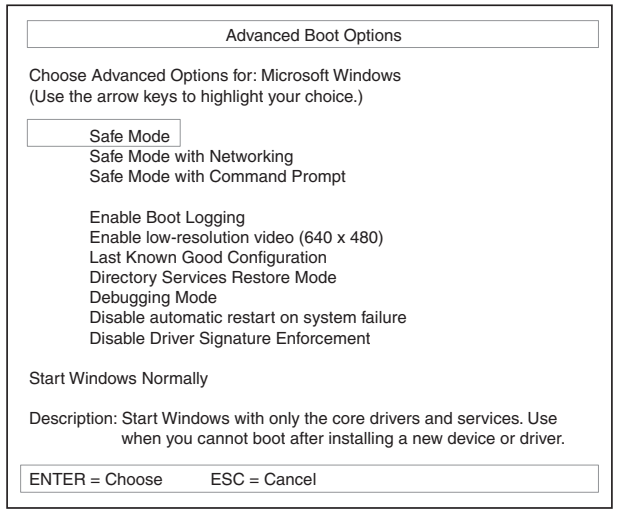
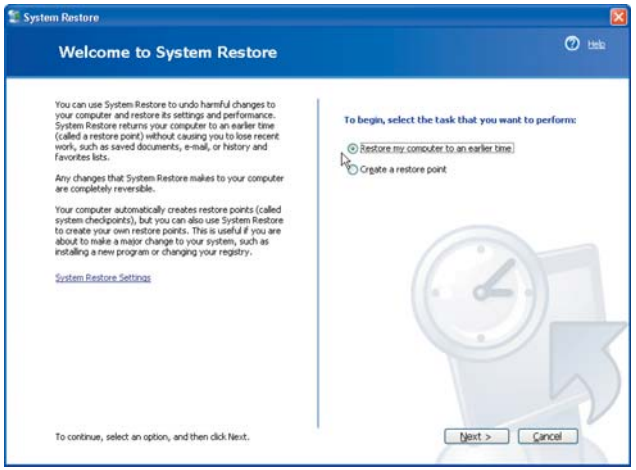

Advanced Boot Options
Choose Advanced Options for: Microsoft Windows
(Use the arrow keys to highlight your choice.)
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Enable Boot Logging
Enable low-resolution video (640 x 480)
Last Known Good Configuration
Directory Services Restore Mode
Debugging Mode
Disable automatic restart on system failure
Disable Driver Signature Enforcement
Start Windows Normally
Description: Start Windows with only the core drivers and services. Use when you cannot boot after installing a new device or driver.
ENTER = Choose
ESC = Cancel

Figure 15-5. Windows Vista **Advanced Boot Options** menu.

Figure 15-6. System Restore gives the option to restore the computer's system settings and performance to a previous point in time or to create a restore point.


System Restore
Welcome to System Restore
Help
You can use System Restore to undo harmful changes to your computer and restore its settings and performance. System Restore returns your computer to an earlier time (called a restore point) without causing you to lose recent work, such as saved documents, e-mail, or history and favorites lists.
Any changes that System Restore makes to your computer are completely reversible.
Your computer automatically creates restore points (called system checkpoints), but you can also use System Restore to create your own restore points. This is useful if you are about to make a major change to your system, such as installing a new program or changing your registry.
System Restore Settings
To begin, select the task that you want to perform:
Restore my computer to an earlier time
Create a restore point
To continue, select an option, and then click Next.
Next >
Cancel

or installing software. If something is done to the system that results in improper operation, the System Restore feature can be used to return the system to its previous state. This is done by selecting **Restore my computer to an earlier time** from the opening screen. System Restore displays a calendar of restore points from which the user can choose, **Figure 15-7.**

Microsoft Windows XP and Vista make an automatic backup of all registry files when you create a system restore point. You can create a system restore point by following the path **Start | All Programs |Accessories | System Tools | System Restore**. The path is the same for Windows XP and Windows Vista.

Recovery Console

The Recovery Console is a last resort recovery utility available in Windows 2000 and XP. Recovery Console is also referred to as "command console" and "repair console." The Recovery Console is used when the problem is so severe, you cannot access the safe mode startup option. Recovery Console is not a GUI utility. It is a text-based command line utility. Commands are issued at the Recovery Console command line prompt. The commands are very similar to the old style DOS commands issued at the DOS prompt. Many of the commands you are probably already familiar with, but there are some new ones. Look at the chart in **Figure 15-8.** The chart is a partial listing of the many commands available in Recovery Console.

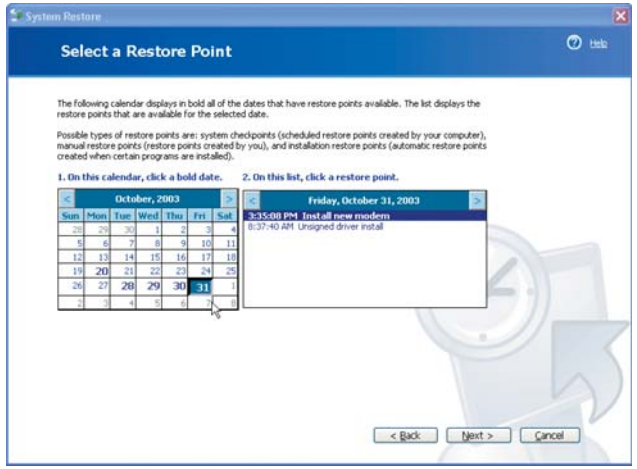

System Restore
Select a Restore Point
Help
The following calendar displays in bold all of the dates that have restore points available. The list displays the restore points that are available for the selected date.
Possible types of restore points are: system checkpoints (scheduled restore points created by your computer), manual restore points (restore points created by you), and installation restore points (automatic restore points created when certain programs are installed).
1. On this calendar, click a bold date.
2. On this list, click a restore point.
October, 2003
Sun Mon Tue Wed Thu Fri Sat
Friday, October 31, 2003
3:35:00 PM Install new modem
8:37:40 AM Unsigned driver install
< Back
Next >
Cancel

Figure 15-7. Several restore points may be available in a single day. These include scheduled restore points created by the computer and restore points created by the user.

Recovery Console looks very much like the Windows command interpreter, but it is not the same. Recovery Console is not installed by default. Unless the computer system has been previously configured to run Recovery Console from the hard disk drive, you must use the installation CD to start the Recovery Console. To do this, insert the installation CD into a bootable CD-ROM drive. You may need to configure the BIOS settings to allow the CD-ROM drive to be the first device in the boot sequence.

When the PC boots to the installation program, select *R* to repair the system and *C* to enter Recovery Console. Selecting *R* will command the Recovery Console to perform an automatic recovery of the system similar to the **Last known good configuration** option. Choosing C displays the Recovery Console command prompt. You can issue commands from the command prompt or copy a missing file from a floppy disk to the operating system directory. The Recovery Console is a last resort utility and should only be used by technicians with advanced troubleshooting experience. Windows Vista has redesigned the Recovery Console into a much more sophisticated utility called the Windows Recovery Environment. It is discussed in the following section.

Windows Recovery Environment

The Windows Recovery Environment (WinRE) is a vast improvement over earlier startup repair utilities developed by Microsoft for their operating systems. It is launched by booting to the Windows Vista installation DVD. A dialog box will prompt you to select the keyboard layout and regional preferences, such as language. The next screen presents an option to perform a system repair and looks similar to that in **Figure 15-9.**

Figure 15-8. Text-based commands available in Recovery Console.

Command	Description
attrib	Clears or sets file attributes.
bootcfg	Used to recover multiboot system failures and to reconfigure the boot.ini file.
cd or **chdir**	Changes directories or folder location.
chkdsk	Checks for and may repair bad disk sectors and checks the surface of the disk.
copy	Copies a file.
del or **delete**	Deletes a file.
dir	Displays the contents of a directory.
disable	Disables a service or driver.
diskpart	Manages the partitions on a disk.
enable	Enables a service or file.
exit	Closes the Recovery Console.
expand	Extracts a compressed file known as a cab file.
fixboot	Writes a new boot sector on a partition.
fixmbr	Repairs the master boot record.
format	Formats a partition, volume, or logical drive.
help	Displays a list of Recovery Console commands.
listsvc	Lists all available services and drivers.
logon	Lists all Windows 2000 and XP systems and lets you log on to one particular system.
md or **mkdir**	Creates a directory or folder.
rd or **rmdir**	Removes a directory or folder.
ren or **rename**	Renames a file.

Look closely in the lower left-hand side of the dialog box and you will see an option to **Repair your computer**. The letter *R* is underlined, which represents the fact that you can simply press the letter *R* on the keyboard to start the repair process. This feature is a standard option in repair scenarios because the mouse might not be working, and you may only have use of the keyboard.

The first dialog box to appear requests you to identify the correct drive or partition to repair. Look at the screen capture in **Figure 15-10** to see the first dialog box as it appears in a repair scenario. The second dialog box to appear prompts you to select the type of repair, as shown in **Figure 15-11.** The five options are as follows:

- ✔ **Startup Repair.**
- ✔ **System Restore.**
- ✔ **Windows Complete PC Restore.**
- ✔ **Windows Memory Diagnostics Tool.**
- ✔ **Command Prompt.**

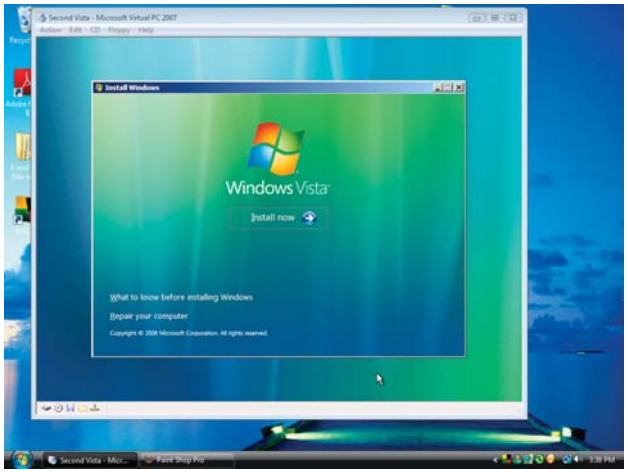


Figure 15-9.
The Windows Recovery Console is accessed by booting to the Windows Vista installation DVD and selecting **Repair your computer**.

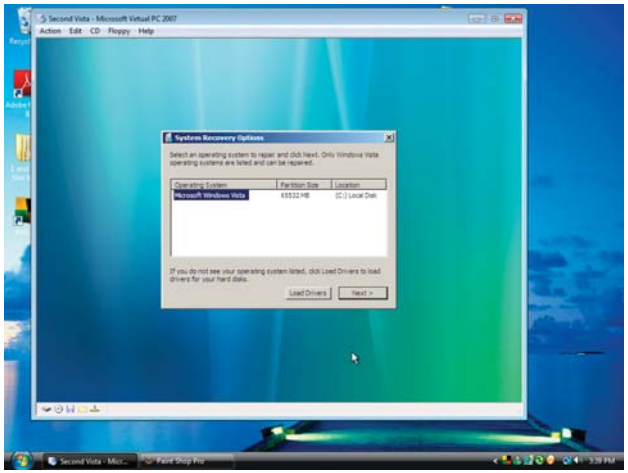
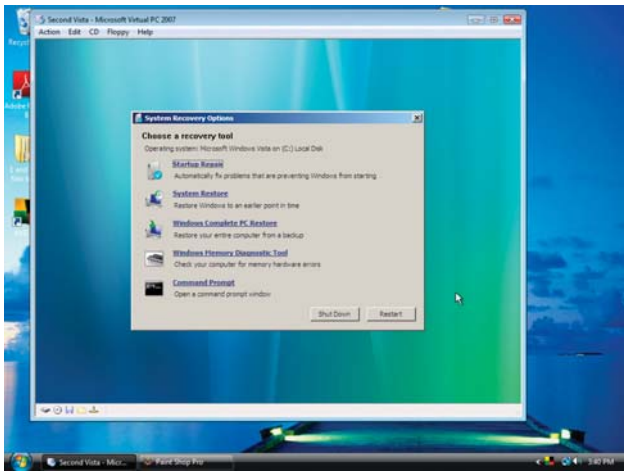


Figure 15-10.
Windows Recovery Environment prompts for the operating system to repair.

Figure 15-11.
Windows Recovery Environment tools.



The **Startup Repair** option searches for and replaces corrupt or missing system files. **System Restore** provides access to the System Restore utility from which you can restore the system to a point in time that the system was working. The **Windows Complete PC Restore** option makes an image of the hard disk drive including files such as the MBR, which normally cannot be accessed or copied without the use of third-party tools. This option is only available in Windows Vista Business, Ultimate, and Enterprise editions. It is not available in the Home versions. It is the most complete restoration option. It replaces the entire collection of operating system files as well as all data. You can even restore the complete system to a brand new computer if the original computer cannot be recovered.

The **Windows Memory Diagnostics Tool** option, of course, loads the Memory Diagnostics Tool, and the **Command Prompt** option provides access to the command prompt from which you can use command line utilities to repair the system.

Some computer manufacturers pre-install System Recovery Tools. To access System Recovery Tools in a pre-installed system you would press [F8] during the boot process and then select **Repair Your Computer** from the **Advanced Boot Options** menu.

Automated System Recovery

The Automated System Recovery (ASR) utility is new with Windows XP. ASR is designed to replace the **Emergency Repair Disk** option used in Windows NT and 2000. The ASR utility automatically restores critical files that were backed up by the Backup utility. The ASR wizard can be accessed through the menu options of the Backup utility and through many third-party troubleshooting utilities.

When ASR is used in conjunction with the Backup utility, it is possible to restore critical system files and data files. The Backup utility is available through **Start | All Programs | Accessories | System Tools | Backup**. The Backup utility can also be accessed by running **NTbackup** from the **Run** dialog box.

Windows Vista continues to offer system backups through the Backup and Restore Center. However, it does not use the acronym ASR when referring to the newest backup and restore system. Be aware that there is a difference between the backup features of the Windows Vista editions. Windows Vista Home Basic and Windows Vista Home Premium do not provide a feature for performing a complete PC backup image. Windows Vista Home basic and Home Premium does include a feature for backing up personal files.

Microsoft System Configuration Utility

With the Microsoft System Configuration Utility (msconfig.exe), also referred to as Msconfig, you can perform a diagnostic startup or select specific services and applications not to load. Using the process of elimination, you can determine which service or application is causing the problem. The System Configuration Utility is used to eliminate items that can cause a problem during the startup of the computer system and after the user logon. This is one of the most common and useful troubleshooting utilities provided by Microsoft as part of the operating system.

Figure 15-12 shows the latest version of the System Configuration Utility used in Windows Vista. When used in troubleshooting startup problems, you can select the **Diagnostic startup** option, which loads only the basic devices and services necessary to start the operating system. You can also select the **Selective startup** option, which provides a more selective diagnostic startup. It allows you to choose between system services and startup items. For a very detailed selection of which services and applications to allow to load and run on the system, additional tabs are provided, such as **Boot**, **Services**, and **Startup**.

This utility is slightly different, depending on the exact operating system and the features associated with that particular operating system. For example, the Windows 95 and 98 System Configuration Utility has tabs named **Win.ini** or **System.ini** to accommodate the win.ini and system.ini files that were used in

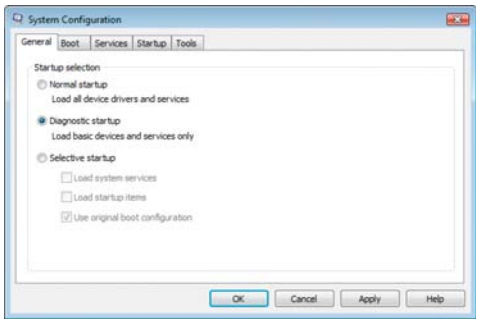


Figure 15-12. Windows Vista System Configuration.

those operating systems, **Figure 15-13.** The Windows Vista System Configuration Utility has several enhancements over previous versions of this utility. For example, the **Tools** tab provides a central and convenient location for some popular tools, such as Event Viewer, Security Center, and Task Manager.

Microsoft System Information

Windows boot problems can be very difficult to diagnose, especially if they are intermittent problems. An extremely useful utility found in the Windows 98 and later versions of the operating system is Microsoft System Information (msinfo32.exe). Microsoft System Information displays detailed information about the hardware and software in the system. **Figure 15-14** shows the window that is displayed after running msinfo32.exe. You can activate it from **Start | Programs | Accessories | System Tools | System Information**, or by typing **msinfo32** at the **Run** prompt.

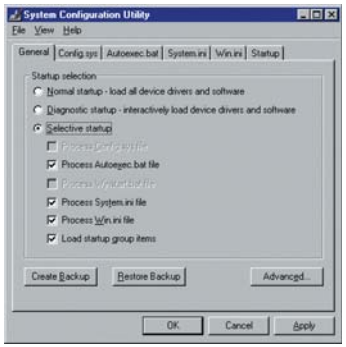


Figure 15-13. Windows XP System Configuration.

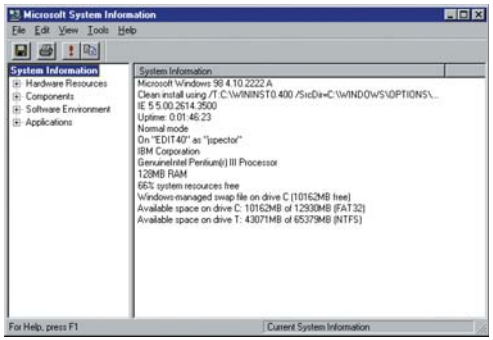


Figure 15-14. Microsoft System Information can be used to find boot problems and other conflicts.

Note that Windows NT does not respond to msinfo32exe. Windows NT is an older operating system and used a set of three emergency recovery disks when problems occurred.

Tech Tip:

Hardware devices, system resources, software, and Internet program settings can be displayed from this location. You can readily determine conflicts in system resources, as well as most startup problems. There is also an online help program. This can assist you when you need to know more about your diagnostics utilities. There are several troubleshooting utilities available through this window. The essentials of some of these utilities will be covered in the next section.

Reinstall the Operating System

If you cannot repair the system using the utilities provided, you will need to reinstall the operating system. This is the very last resort to recovering from a system startup failure. When reinstalling the operating system, first try to perform a system upgrade. This will allow you to retain the data files that reside on the hard drive. Performing a new installation rather than a system upgrade wipes out all existing files on the hard drive, thus losing all data files.

Some problems can be intermittent and be a hardware problem related to a loose connection or excessive heat. For example, heat could slowly build up inside a computer caused by partially blocked airflow path, resulting in over heating the memory modules. Once the memory module has overheated, the system locks up. Always be aware of "What happened last" when troubleshooting a computer.

Tech Tip:

Windows Diagnostic Utilities

Most Microsoft operating systems carry the same troubleshooting utilities. You need to become familiar with these utilities to save time when troubleshooting a system problem. Let's see how they might be helpful.

Dr. Watson

Dr. Watson is a standard Microsoft troubleshooting utility that is used to diagnose software fault problems. Dr. Watson collects information about the computer system during and just before a software application fault. It tracks down the program that caused the fault and reports the part of the memory and the program in which it occurred. This information can be used when contacting product support.

Dr. Watson does not load automatically. To activate Dr. Watson, click **Start | Run**, type **drwatson**, and then click **OK**. The Dr. Watson diagnostic program will appear as an icon in the system tray (bottom right taskbar area). You can then

right-click the icon to open it. You can also access Dr. Watson, as mentioned earlier, through **Start | Programs | Accessories | System Tools | System Information**, click on the **Tools** menu, and then choose **Dr. Watson**.

By accessing **View** from the menu and selecting **Advanced View**, you can view the drivers, startup programs, and many more items, **Figure 15-15.** Dr. Watson can also write to a log to save errors and the descriptions of faults. These descriptions can be used when contacting support. Dr. Watson cannot diagnose a system hang or lockup condition. Starting with Windows Vista, Dr. Watson has been replaced with Problem Reports and Solutions. This utility is discussed later in this section.

DirectX Diagnostic Tool

DirectX is a software development tool used for multimedia applications. It allows programmers to directly access many of the built-in features of Windows. A poorly written program using DirectX can cause severe system hangs or crashes. The DirectX Diagnostic Tool looks at every DirectX program file on the computer, **Figure 15-16.** You can look for non-Microsoft approved program labels here. If it is Microsoft approved, you should not have a problem. That cannot be said for other programmers' tools. DirectX program files are abundant. They are used for game development and all types of multimedia programs. The Directx Diagnostic Tool is still incorporated into Windows Vista, but it is much more sophisticated than earlier versions.

System File Checker

The System File Checker (sfc.exe) can be run to check for corrupt, changed, or missing files from Windows-based applications. See **Figure 15-17.** It can also be used to restore system files. To start the System File Checker program in Windows versions earlier than Windows XP, select it from the **Tools** menu in the **Microsoft System Information** utility, or type **sfc** in the **Run** dialog box. In Windows XP, you can access the system file checker by typing **sfc** at the command prompt. The responsibilities of System File Checker are incorporated directly into the Windows Vista Resource Checker, but it can still be run from the command prompt with administrator rights using the **sfc** command.

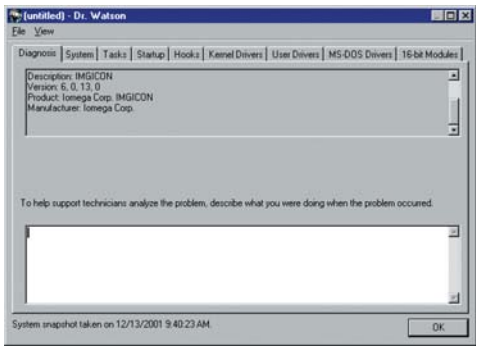

(untitled) - Dr. Watson
File View
Diagnosis System Tasks Startup Hooks Kernel Drivers User Drivers MS-DOS Drivers 16-bit Modules
Description: IMGICON
Version: 6. 0. 13. 0
Product: Iomega Corp. IMGICON
Manufacturer: Iomega Corp.
To help support technicians analyze the problem, describe what you were doing when the problem occurred.
System snapshot taken on 12/13/2001 9:40:23 AM.
OK

Figure 15-15. The advanced view in Dr. Watson can be shown by selecting the **View** menu and selecting **Advanced View**. Running Dr. Watson places an icon in the system tray. You can activate the program from there.

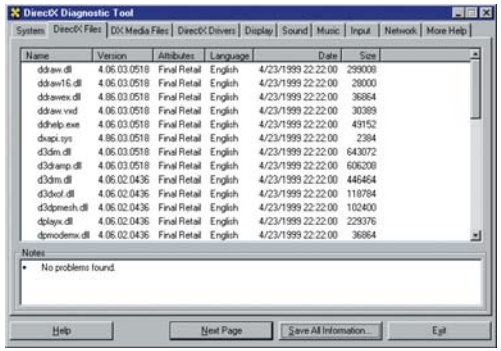


Figure 15-16. The DirectX Diagnostic Tool checks for problems with DirectX files. This check shows no problems.

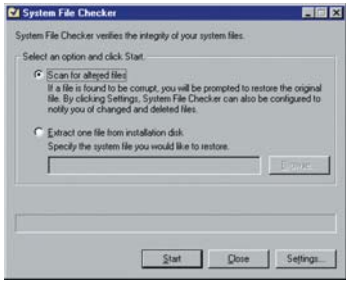

System File Checker
System File Checker verifies the integrity of your system files.
Select an option and click Start.
Scan for altered files
Extract one file from installation disk
Specify the system file you would like to restore.
Start
Close
Settings...

Figure 15-17. System File Checker can by used to check the integrity of system files.

Windows Report Tool

The Windows Report Tool is a utility that allows the PC system settings to be copied and sent to technical support for evaluation. Of course, a modem connection is needed and the system must be bootable. **Figure 15-18** shows the **Windows Report Tool** dialog box as it appears in Windows 98 and Me. Text box areas are provided for you to report information about the error.

Figure 15-19 shows the **Error Reporting** dialog box available in Windows XP. In Windows XP, you can choose to report errors generated by the Windows operating system or by other programs installed on the computer. Some programs may generate an error report each time they are launched or closed. If you find the automatic generation of an error report annoying, there is an option to disable it. The Error Reporting utility can be accessed through the **System Properties** dialog box in Windows XP, **Figure 15-20.** The complete path to the Error Reporting utility is **Start | Settings | Control Panel | System | Advanced | Error Reporting**.

Figure 15-18. Windows Report Tool as it appears in Windows Me. Pay particular attention to the text box areas that allow user input describing the problem.

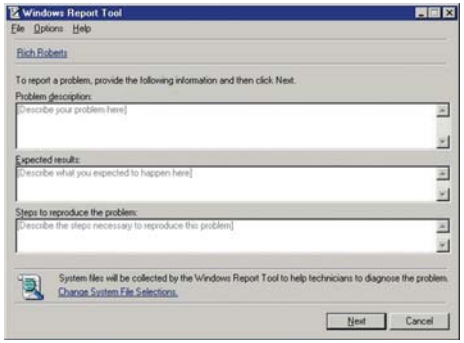
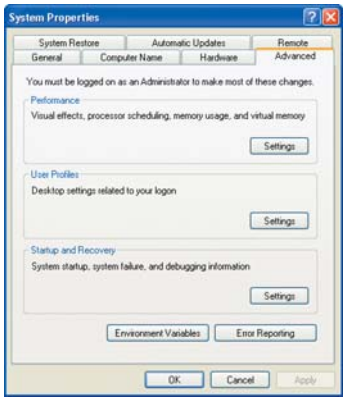

Windows Report Tool
File Options Help
Rich Roberts
To report a problem, provide the following information and then click Next.
Problem description:
[Describe your problem here]
Expected results:
[Describe what you expected to happen here]
Steps to reproduce the problem:
[Describe the steps necessary to reproduce this problem]
System files will be collected by the Windows Report Tool to help technicians to diagnose the problem.
Change System File Selections.
Next
Cancel

Figure 15-19. An example of the **Error Reporting** dialog box in Windows XP.

Figure 15-20. Look at the **Error Reporting** button in the lower-right area of the **System Properties** dialog box. This is used to access the **Error Reporting** dialog box in Windows XP.



Windows Vista uses the Problem Reports and Solutions feature to serve as the same function as Windows Report Tool. It is discussed later in this section.

Registry Editor

You can also manually view and modify registry contents manually by running either regedit.exe or regedt32.exe. Regedit.exe is a 16-bit version of the registry editor and regedt32.exe is the 32-bit version. Windows Vista does have a version of both available. Windows XP will run either editor, but the preferred registry editor to make changes is regedt32.exe.

Microsoft states that, in general, you should not edit or modify the contents of the system registry. There are times when Microsoft provides step-by-step instructions as to how to modify the contents of the registry using these utilities to repair a problem. Never simply use trial and error methods when working with a registry. The contents of the registry are critical. An improper modification can disable the computer operating system requiring a complete reinstallation of the system files and possible loss of important data. Microsoft has an extensive article on registry editing and recovery at the following Web site links:

- ✔ http://support.microsoft.com/kb/256986.
- ✔ http://support.microsoft/kb/322756.
- ✔ http://support.microsoft.com/kb/307545.

You should never attempt to repair the registry files directly. An error made in the registry files can render the computer system inoperable. You may have to completely reinstall the system onto a clean hard drive. Simply loading the software over the corrupt registry would do no good. The new installation would inherit the previous corrupt settings.

Event Viewer

The Event Viewer in Windows 2000 and XP allows you to view the application, security, and system log files. These log files are named AppEvent.Evt, SecEvent.Evt, and AppEvent.Evt and are only viewable through the Event Viewer program. Each log can be viewed in chronological order or by categories such as event and user. Since the Event Viewer log files retain a history of events that have occurred on the PC, it can be a very valuable troubleshooting tool. For example, users typically will not want to reveal information about installed software such as games, especially if gaming software is against company policy. A technician can quickly view a list of software changes and obtain objective data that can be used to identify possible causes of system problems.

Further enhancements were developed for Event Viewer in Windows Vista. Look at **Figure 15-21.** The Event Viewer is a centralized depository of various logs that were kept separate in early versions of Windows operating systems. Event logs relating to system setup and configuration, applications, security, and more can be accessed and grouped into summaries such as Error, Warning, Information, and Audit success. You can use the mouse to select specific types of event and expand the list. You can then select individual events and look at them in detail, as shown in **Figure 15-22.** Notice that more information about the event

Figure 15-21.
Windows Vista Event Viewer.

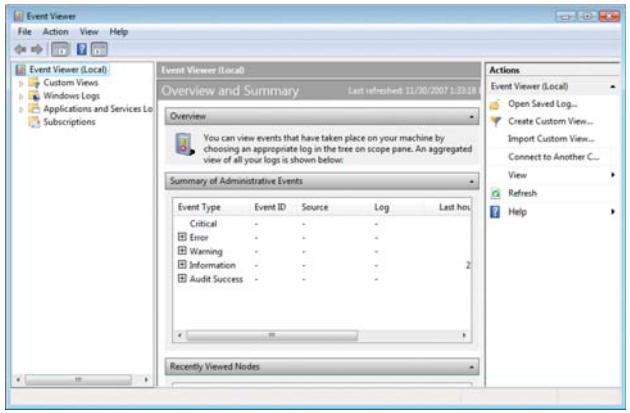
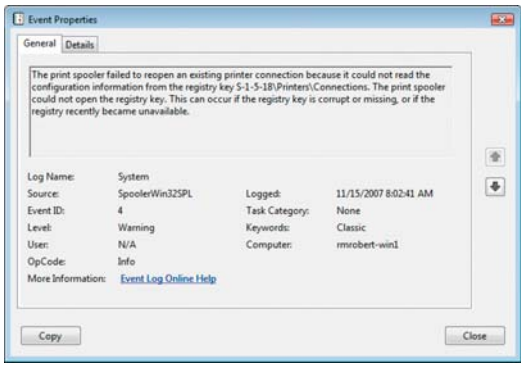


Figure 15-22.
Detailed information about an event is shown in the **Event Properties** dialog box and is accessed by double-clicking the event.


Event Properties
General
Details
The print spooler failed to reopen an existing printer connection because it could not read the configuration information from the registry key S-1-5-18\Printers\Connections. The print spooler could not open the registry key. This can occur if the registry key is corrupt or missing, or if the registry recently became unavailable.
Log Name: System
Source: SpoolerWin32SPL
Logged: 11/15/2007 8:02:41 AM
Event ID: 4
Task Category: None
Level: Warning
Keywords: Classic
User: N/A
Computer: rmrobert-win1
OpCode: Info
More Information: Event Log Online Help
Copy
Close

can be accessed through the **Event Log Online Help** option. To find more about the extensive capabilities of the Windows Vista Event Viewer use Windows Vista Help and Support.

Log files are created as ASCII text files. They are used to record events that take place or to collect information about hardware and software systems. There can be many different log files on a computer system, not just the ones discussed in this section. These logs are created because many software and hardware manufacturers write their own log file collection programs to assist them (and you) in determining problems that may have occurred during the installation of their hardware or software package. The log files can also be used to relay information to technical support personnel by e-mail or telephone. Sometimes these files can also be accessed remotely by technical support personnel.

Remote Assistance

Remote Assistance was introduced with Windows XP. It allows a user to invite another user to access their computer and assist them in repair. The user needing help sends an e-mail invitation to another person, such as a technical support person. Technical support can then repair the system while they chat with the user.

Remote Assistance should not be confused with Remote Desktop. Remote Desktop allows a user to connect directly to their computer from another location. For example, a user could connect to their office computer from their home computer. The user would have complete control over their office computer just as if they were sitting at its keyboard. Remote Assistance is a temporary connection, and a person must be present at both locations.

Figure 15-23 shows the remote connection options listed in the **System Properties** dialog box under the **Remote** tab. Both Remote Assistance and Remote Desktop are available in Windows XP Professional and Windows Vista, but only Remote Assistance is available in Windows XP Home Edition.

Windows Vista Problem Reports and Solutions

The Windows Vista Problem Reports and Solutions utility, **Figure 15-24,** identifies problems as they occur on the system and can be used to automatically find solutions. Problems are automatically reported to Microsoft via the Internet. If a solution is known, it is sent to the computer and is posted in a window as a solution. A complete history of all problems and solutions can be archived for future use and diagnostics. This is a great improvement over previous versions of error reporting utilities. The path to this utility is **Start | Maintenance | Problem Reports and Solutions**.

Figure 15-23. Two remote access programs are available in Windows XP Professional: Remote Assistance and Remote Desktop. The Windows XP Home addition only includes Remote Assistance.

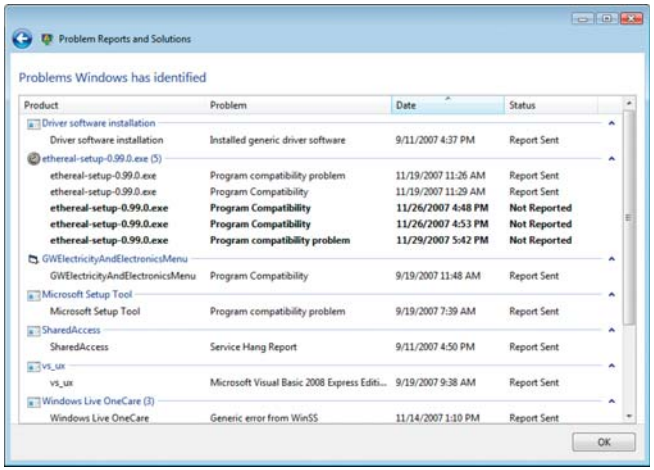


Figure 15-24. The Problem Reports and Solutions utility keeps a listing of all the problems Windows Vista has identified on the system, including a description of the problem, the date it was identified, and whether or not a report was sent to Microsoft.

Windows Vista Reliability and Performance

Windows Vista Reliability and Performance utility is a new addition to the Microsoft Computer Management console. **Figure 15-25** shows the **Reliability and Performance** option in the left-hand pane and the program in the center pane. Notice that the Reliability and Performance utility displays the current condition of the CPU, disk drive(s), network adapter, and memory. The options for this utility are extensive and too much to cover in a short section. To learn more about the Reliability and Performance utility, use Windows Vista Help and Support.

Windows Vista Memory Diagnostics Tool

Memory problems can be difficult to identify because they can occur intermittently. For example, if a computer slowly overheats after an extended period of time, RAM could stop working or cause software program errors. Often, a technician may do a complete reinstallation of the operating system only to have a random error occur once more. Microsoft Vista now includes the Memory Diagnostics Tool, which diagnoses memory chip problems. If the Memory Diagnostics Tool detects a problem with a section of RAM, it automatically restricts the use of the RAM cell locations to avoid using the defective memory section. This allows the computer to be used until the RAM is replaced.

To start the Memory Diagnostics Tool, go to **Start | All Programs | Administrative Tools**. Right-click **Memory Diagnostics Tool** and select **Run as administrator** from the shortcut menu. You will be prompted that Windows needs your permission to continue. Click **Continue** to grant permission.

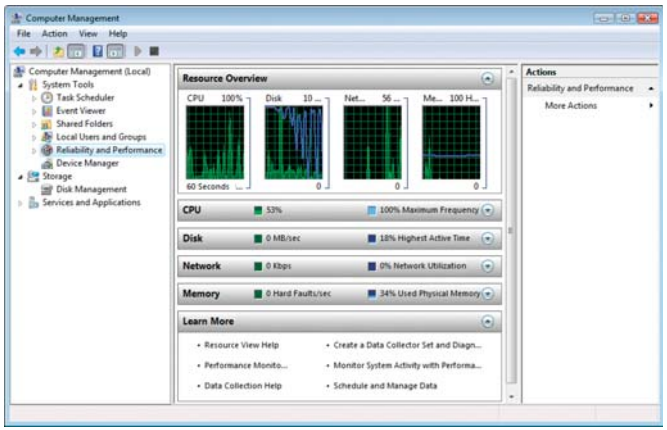


Figure 15-25. Windows Vista Reliability and Performance utility.

You can also start the Memory Diagnostics Tool from the command line. To do this, right-click **Command Prompt** in the **Start menu**. Select **Run as administrator** from the shortcut menu. You will be prompted that Windows needs your permission to continue. Click **Continue**. Enter **mdsched** at the command prompt.

Figure 15-26 shows the **Windows Memory Diagnostics Tool** dialog box. Notice that the test can be performed immediately or scheduled to run the next time the computer is started. The **Windows Memory Diagnostics Tool** in progress looks similar to that in **Figure 15-27.** Notice that the status of the memory diagnostics appears on the screen in text mode, not graphic mode. The progress of the tests is presented as a bar graph and as a numerical percentage. Any problems identified are also presented on the screen.

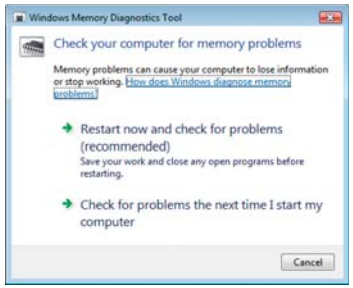
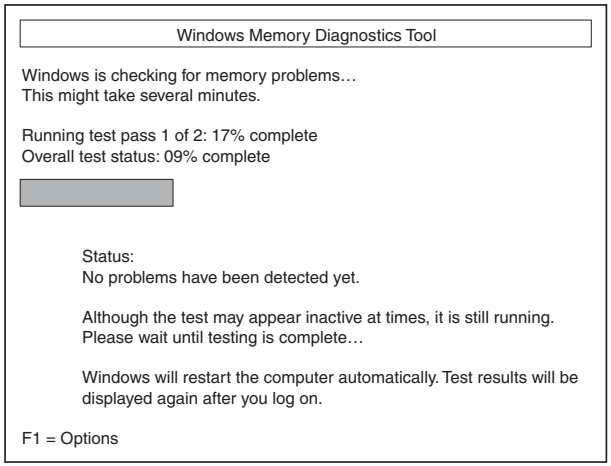

Windows Memory Diagnostics Tool
Check your computer for memory problems
Memory problems can cause your computer to lose information or stop working. How does Windows diagnose memory problems?
Restart now and check for problems (recommended)
Save your work and close any open programs before restarting.
Check for problems the next time I start my computer
Cancel

Figure 15-26. The Windows Memory Diagnostics Tool is a new utility introduced with Windows Vista.

Figure 15-27. A recreation of the Windows Memory Diagnostics Tool in progress.


Windows Memory Diagnostics Tool
Windows is checking for memory problems…
This might take several minutes.
Running test pass 1 of 2: 17% complete
Overall test status: 09% complete
Status:
No problems have been detected yet.
Although the test may appear inactive at times, it is still running.
Please wait until testing is complete…
Windows will restart the computer automatically. Test results will be displayed again after you log on.
F1 = Options

The Windows Memory Diagnostics Tool can also be run from the **Memory Diagnostics Tool** option on the Windows Vista installation DVD.

Boot Sequences

The computer boot sequence is very similar in all the Windows NT-based operating systems (Windows 2000 and Windows XP) and Windows Vista. However, the boot sequence of these operating systems is very different from Windows 98 and earlier operating systems. A good understanding of the startup process is an essential part of troubleshooting. It is, therefore, imperative that you study the boot sequence of all standard operating systems and compare the differences. One way to accomplish this is to study the programs associated with the boot disk created for each system. The boot disk contains the files necessary to boot the computer as well as some of the various enhancement files. Not all files on a boot disk are necessary for booting the system. Information about a system boot sequence and boot files are usually contained in the readme.txt file of the installation discs. Always read the readme.txt files of the operating system you are installing for the first time.

The following table compares the boot sequences of the various Windows operating systems. Notice that they are all similar in that they begin with the POST.

Windows 95, 98, and Me	Windows 2000 and XP	Windows Vista
POST	POST	POST
io.sys	Initial startup phase	Initial startup phase
msdos.sys	Boot loader phase	Windows Boot Manager phase
config.sys	Detect and configure hardware phase	Windows Boot Loader phase
command.com	Kernel loading phase	Kernel loading phase
autoexec.bat	Logon phase	Logon phase

Power-On-Self-Test (POST)

When a computer has power first applied to the motherboard by pressing the on power switch, the BIOS or EFI will start the boot process by performing a quick check of hardware components and verifying that all hardware devices listed in the BIOS configuration database are present and appear to be in working order. The BIOS configuration settings are typically automatically detected or manually modified when the computer is first assembled and started the very first time. The BIOS typically has a default configuration that will usually start most computers without a problem, but not always. Some BIOS configurations require technician modification. The hard disk drive is automatically detected and configured by the BIOS and typically does not need to be modified by the technician. All configuration data is then stored in the CMOS memory.

The BIOS is independent from the operating system. All systems today use either BIOS or EFI as the first computer software routine to run on the computer. Since the POST is independent of the operating system, it is safe to assume that you have a hardware problem if the computer fails during the POST or the POST generates an error message or a series of beeps. You can research the error message or beep codes at the BIOS or motherboard manufacturer Web site. You can also do an Internet search using the contents of the error message as the key terms. The following is a partial list of the system hardware checked during the POST:

- ✔ CPU system clock.
- ✔ CPU registers.
- ✔ Keyboard controller.
- ✔ Video controller.
- ✔ RAM.
- ✔ Disk controllers.
- ✔ Motherboard bus.
- ✔ Adapter card ROM.

The POST can only display error messages after the video has been tested and verified. The system can fail or lock up before the video has been verified and thus give no screen error message.

When POST is complete, some adapters such as video cards or hard disk drives may carry out their own firmware diagnostics routine that is built into the device. This is independent from BIOS diagnostics.

The Extensible Firmware Interface (EFI) is a new approach to the BIOS system. The original BIOS program was first developed in the late 1970s. Before BIOS, each computer manufacturer had to have a matching operating system designed especially for that computer. After the BIOS was developed, you could run a variety of operating systems on the same computer. The BIOS was responsible for linking the communications between the operating system and the PC hardware. EFI was first introduced by Intel, but now a large group of computer hardware manufacturers are involved with creating a set of standards of design for EFI. The group organization is the United EFI (UEFI). EFI can be installed to work directly with BIOS or as a replacement for BIOS. EFI is required on computers that wish to use a new file system directory structure referred to as GUID. In the future, EFI is expected to replace BIOS.

EFI was not supported by the Windows Vista operating system at the time of Windows Vista's original release. However, the Windows Vista service pack 1 does include support for EFI system. Apple MAC OS X first started support of EFI in 2006. EFI is also supported by various Linux systems such as Red Hat and Novell SUSE. The Intel Itanium processor is designed to support EFI as well. Microsoft Windows Server 2003 was the first Microsoft operating system to support EFI. Hewlett Packard (HP) also supports EFI on their HP-UX servers, which are Unix-based systems.

Traditional BIOS is limited in size and typically has less than 1 MB of ROM. It also uses 16-bit drivers. EFI is not limited in size and can load 32-bit and 64-bit drivers before the operating system is loaded. EFI can also load and run applications during the POST without the loading of an operating system. For example, a diagnostic utility or disaster recovery tool, or even a virus check program, can be run before the operating system is actually loaded. This is an extreme difference when comparing BIOS- to EFI- based systems.

BIOS is not governed by any collective organization, and there is no one set of standards controlling the design of BIOS code. The United EFI (UEFI) organization has designed the EFI to be totally vender neutral. This means no one operating system or no one BIOS manufacturer can control the firmware coding. All source code is open and shared so that all software and hardware designers have full access to the EFI coding. Expect the transition from BIOS to EFI to be gradual, not abrupt. EFI motherboards also support traditional BIOS.

Initial Startup Phase

In the initial startup phase, the POST completes and then looks for the boot device where the master boot record (MBR) is stored. The BIOS configuration determines the order for the computer system to locate the next boot device. The boot device could be the floppy drive, the hard disk drive, the CD or DVD drive, or the USB Flash drive. The exact order can be changed in the BIOS Setup program and stored in the CMOS memory. In general, the computer uses the hard disk drive as the boot device. Exceptions are when a floppy is used to startup the computer or when an installation CD or DVD is used to install an operating system or for system recovery.

After identifying the location of the MBR, the BIOS loads the MBR into RAM. For Windows 95, 98, and Me, the BIOS then loads the io.sys file into RAM. You should recall that the io.sys file contains generic drivers necessary for communicating with hardware devices such as the monitor, floppy drive, hard drive, and keyboard. This io.sys file then loads the file allocation table (FAT) into RAM. The FAT is a table of all the files on the hard drive along with their attributes and locations. For Windows 2000 and XP, the BIOS loads the ntldr file into RAM, and for Windows Vista, it loads the Windows Boot Manager (bootmgr).

Keep in mind, you cannot use a non-bootable CD, DVD, or floppy to start the computer. When a non-bootable media is encountered during the boot sequence, an error message will appear on the screen. Some possible errors include the following:

- ✔ Non system disk.
- ✔ Missing Ntloader (ntldr).
- ✔ Hard disk errors.

In an EFI system, a GUID Partition Table (GPT) is used instead of an MBR to locate partitions on a physical disk(s). This table overcomes the partition limitations imposed by the MBR. Before GPT, Microsoft operating system partitioning was based on the limitations of the MBR. Partitions could consist of four primary partitions or three primary partitions and one extended partition subdivided into logical partitions. This is an archaic partitioning system, which evolved from the DOS file system. The maximum number of partitions that can be supported by the Microsoft operating systems is 128. Since the GPT does not have the same limitations of MBR-based partitions, you can have almost an unlimited number of partitions using GPT. EFI does not require a GPT partition and can be used with a partition system based on MBR. Also, EFI can use a disk system that contains both GPT and MBR partitions.

Since the rest of the boot sequence is different for each of the three types of operating systems, the rest of this section is organized by operating system. Each operating system boot sequence discussion continues from the initial startup phase to the last phase for that particular operating system.

Windows 95, 98, and Me

In the previous stage, the io.sys file was loaded into memory, and the io.sys file loaded the FAT into memory. With the FAT in memory, the io.sys file can locate the msdos.sys file. The msdos.sys file is a text file that contains references to items such as where the Windows files are located and options for displaying the boot menu.

The io.sys file then processes the config.sys, command.com, autoexec.bat and win.com files. The Windows startup process only loads the config.sys file and then the autoexec.bat file, if they are required for support of legacy programs. With these operating systems, Microsoft started moving away from the use of config.sys, autoexec.bat, and the win.ini and system.ini files. The win.ini and system.ini files were used with earlier versions of Windows and stored hardware and software information. These files were replaced with the system registry. The system registry is a database that stores information about the hardware and software systems. The registry is continually referenced by the operating system and software programs. The autoexec.bat, config.sys, command.com, and io.sys have been renamed for Windows 98 by changing the file extensions to .dos. For example, io.sys in Windows 98 is now called io.dos.

The config.sys and autoexec.bat files are not required for Windows 95, 98, and Me but are still available to maintain downward compatibility with legacy software programs and drivers.

After autoexec.bat loads, the win.com file loads. Win.com then loads the Windows kernel (krnl386.exe), the graphic device interface (gdi.exe), and user.exe. The krnl386.exe is the kernel file or core program of the operating system. (There is also a krnl286.exe, which was used with earlier models of the operating system.) It manages the processor functions and system resources such as memory DMA channels, IRQs, and port functions. It also loads programs, schedules processor events, and controls the actions of the CPU. The user.exe file is designed to allow the user to manipulate the icons, windows, and elements that make up the user interface. The gdi.exe is the graphic device interface. It is responsible for displaying the screen images used as the interface between the user and the operating system. All three files are located in the directory structure under **Windows | System**.

After these three program files are processed, the logon window appears. The user logs on, and the system processes the user's individual settings.

The system registry contains two main files called system.dat and user.dat. The system.dat file contains information that is specific about the computer. The user.dat contains information about the user. A PC may have multiple users, thus there can be multiple user.dat files containing information about each specific user. Such user information would include, but not be limited to, desktop layout preferences and specific documents created by the user.

Windows 2000 and XP Boot Sequence

Windows 2000 and Windows XP are designed on the NT operating system kernel, not the traditional Windows 95/98 operating system kernel. However, their outward appearance is remarkably similar.

As with the other systems covered so far, these systems start with the POST, load the BIOS program, and look for the boot sector as well as the MBR. Then, Windows 2000 and XP follow the NT system. Once the BIOS has loaded the ntldr file into RAM, it turns control over to it for the boot loader phase. During this phase, ntldr loads the program startup files from the boot sector. Part of

loading the startup files is the detection of the preferred operating system. This information is stored in the boot.ini file. Windows 2000 and XP, like NT, allow for the existence of more than one operating system. They will coexist with Windows 95, Windows 98, Windows NT, MS-DOS, and OS/2.

Note that in a BIOS-based system, the operating system provides a boot manager to select which operating system to boot to after the POST has been completed. Often there are compatibility issues when multiple operating systems reside on the same computer and use a boot manager designed by one of the operating system, such as Microsoft or Linux. The EFI has designed and implemented a boot manager that allows the selection of the operating system to load during the POST period. This will hopefully prevent incompatibility issues caused by the operating system designing the boot manager rather than the EFI standard implementing the operating system boot manager.

Once Windows 2000 or XP is selected as the operating system, ntldr calls the ntdetect.com file. This file detects the hardware in the PC system. After the hardware detection is complete, the boot process loads the operating system kernel called ntoskrnl.exe and the hal.dll. The hal.dll is the hardware abstraction layer. The Windows 2000 and XP operating systems do not allow software programs to gain direct access to the system hardware the way that traditional Windows programs allow. The hal.dll is a machine language program that serves as the go-between for software and hardware. The hal.dll makes it possible for the computer system to be hardware and device independent. It supports many different CPU platform designs. In other words, the PC does not have to be an IBM clone. It could use a processor such as Digital's Alpha processor. The ntoskrnl.exe file is the heart of the operating system. It initializes the hardware system and drivers. It controls and oversees the entire operating system and the processing of instructions and files.

The entire boot process is not considered complete until you log on with the [Ctrl] [Alt] [Delete] key combination. Once you log on, the system turns to the user mode of operation. There are two modes of operation: user mode and kernel mode. ***Kernel mode*** oversees the system resources and processor actions. This is an automatic mode requiring no user intervention. ***User mode*** is the actual user interface with the operating system. It is very restrictive in the sense that many areas are not accessible by the user or user programs. This environment is what makes NT-based operating system such a stable system as compared to other earlier Microsoft Windows products. The stability is due to software and users not being allowed to manipulate hardware resources and features.

kernel mode
automatic Windows NT mode of operation that oversees the system resources and processor actions.

user mode
the actual user interface mode for the NT-based operation system. It is very restrictive and many areas are not accessible by the user or user program.

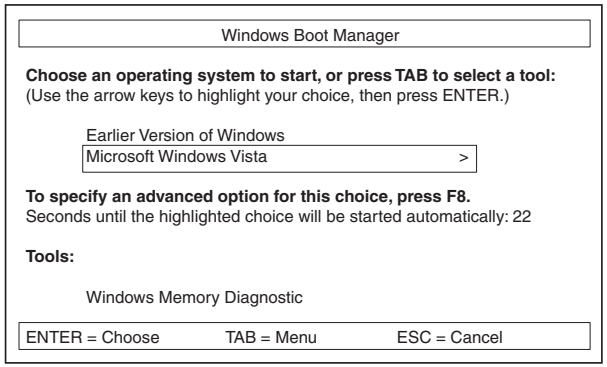
Windows Vista Boot Sequence

In Windows Vista, ntldr has been replaced by the Windows Boot Manager (bootmgr) and Windows Vista Boot Loader (winload.exe). Ntdetect is incorporated into the kernel. Windows Vista also uses Boot Configuration Data (BCD) in place of the boot.ini file, which is used by previous versions of Windows. This section begins with the Boot Manager phase.

Boot Manager phase

The Boot Manager (bootmgr) is used to select which operating system to load when more than one operating system is present on a computer. If more than one operating system is installed on a computer, a screen similar to the one in **Figure 15-28** will appear. The Windows Boot Manager screen does not appear if only one operating

Figure 15-28.
The Windows Boot Manager menu will appear by default if there are multiple operating systems on the computer.


Windows Boot Manager
Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)
Earlier Version of Windows
Microsoft Windows Vista >
To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 22
Tools:
Windows Memory Diagnostic
ENTER = Choose
TAB = Menu
ESC = Cancel

system is installed on a computer. However, the Boot Manager still runs even if it does not appear on the display. The default for the boot manager is 30 seconds, but the delay is reduced to approximately 2 seconds when only one operating system is present. It is during this two-second interval that the [F8] key can be pressed to interrupt the boot process causing the **Advance Boot Options** menu to appear. The **Advanced Boot Options** menu is similar to the one in Figure 15-5.

If you do not press [F8] within the two seconds after completion of the POST, the operating system will quickly load the Windows Boot Loader (winload.exe), the Kernel (ntoskrnl.exe), and the Session Manager (smss.exe), which results in the familiar Windows graphical user interface. The **Advanced Boot Options** menu cannot be accessed once the computer reaches this point. You must restart the computer to access the **Advanced Boot Options** menu with the [F8] key. You may start pressing the [F8] key before POST is finished. This will usually automatically start the **Advanced Boot Options** menu. The Boot Manager then passes control to the Boot Loader.

Boot Loader phase

In this phase, the Windows Boot Loader (winload.exe) first loads the kernel (ntoskrnl.exe) into RAM, but does not execute it yet. Next, the hardware abstract layer file (hal.dll) is loaded into RAM as well as the system registry hive. Certain key services are started to support various device drivers that are required during the boot process. Lastly, the kernel (ntoskrnl.exe) is executed and takes over operation of the computer system.

Kernel loading phase

After the kernel (ntoskrnl.exe) is executed, the kernel and hardware abstract layer (hal.dll) work together to communicate with software applications, drivers, and hardware. Driver files that do not require user security clearance are typically loaded. For example, the driver and services required to minimally run the printer is loaded at this time.

Now the kernel and hardware abstract layer work together to process information stored in the registry which will be required to complete the boot process. The kernel creates a new registry key which contains information about

the drivers and devices loaded so far and through the rest of the boot operation. This information is used for the **Last known good configuration** boot option when troubleshooting the system or attempting to recover from a system failure. The kernel then loads the Session Manager (smss.exe).

Session Manager phase

In this phase, the boot process switches from text mode to graphic mode. A progress bar appears at the bottom of the screen. The session manager continues to run in the background until the computer is shut down.

The Session Manager starts and runs an abbreviated version of Chkdsk and determines if the system volumes and partitions are in working order. The Session Manager is also responsible for loading the page file or virtual memory. The page file supplements the amount of RAM installed on the computer.

Microsoft does not allow third-party venders' software applications to directly access hardware and certain operating system files. But when access is needed by the third-party software applications, the Session Manager manages the activities. If the startup process fails here, you will see a Microsoft system blue screen error. Recall that a blue screen error is a full-screen text message describing the error on a plain, blue background. There will be a cryptic error code that can be used to conduct a search at the Microsoft Web site to find the most likely cause. Microsoft has a very extensive collection of troubleshooting information at their TechNet Web site. The last phase of the startup process is called the *logon phase*.

Logon phase

In this phase, the windows logon file (winlogon.exe) is executed, and the Windows Logon dialog box appears. A user typically enters his or her logon name and password to proceed to the operating system desktop.

After a successful logon, the lsass.exe file loads and runs. This file is the Local Security Authority (LSA). Then, the service subsystem file, services.exe loads and runs. The exact services loaded and started is determined by the computer's configuration and the user's credentials. Only the services the user is allowed to access will start. If there is only one default user and the computer is not connected to a network with a server, the user will be able to access and run all services for the computer. If a user has a limited account, they will only be able to run services allocated by the system administrator.

Startup programs are loaded and run at this point. Any problems such as the computer freezing up or a very long delayed appearance of the user desktop are associated with the startup files and services. If a computer user installs many programs over a period of time, the appearance of the desktop after completing logon will take more time.

After a successful logon, the boot process is considered a success. The registry is updated and will become the registry reference for the "Last known good configuration." A failure of the system after logon is usually a sign of a failed service or a software startup application.

One of the best utilities for analyzing failures after logon is the System Configuration Utility (msconfig.exe). You can select and isolate services and software applications that might be causing the problem.

Linux Boot Sequence

Some common versions of Linux are SUSE, Xandros, Red Hat, Caldera, and Debian. All have graphical user interfaces available and appear similar to the Windows screen display.

Linux is similar to the other systems in that a POST is performed and a BIOS routine is loaded. It is common to boot from a floppy disk when using Linux, but you may also boot from the hard drive. Like any typical startup operating system, after the initial system startup, the Linux operating system takes over. Linux uses a boot manager called *lilo*, which stands for *Li*nux *lo*ader. Lilo looks at the configuration file called lilo.conf to detect operational information. The lilo boot manager allows the user to select other operating systems when more than one exists on the hard drive. Linux operating systems can coexist with Microsoft Windows operating systems. Once the Linux kernel loads, the system runs the init program. The init is the system initialization, similar to DOS or Windows. All the system processes, such as the keyboard, mouse, and network connections, require initialization.

Data Recovery Techniques

Many times data on a nonfunctioning hard drive is not actually lost, although it cannot be directly accessed. Think about the causes of failure for a hard drive. They include the electronics board mounted on the hard drive, the mechanical parts inside the drive, or simply a boot sector failure. If you can still see the drive directory on drive C when using a boot disk, chances are excellent for recovering the data.

One of the most common ways to recover data is with software. There are a number of third-party programs out there designed to read disks that show as bad. **Figure 15-29** shows a disk being accessed by Norton Disk Editor. It can examine the disk and display the sectors in your choice of ASCII, binary, or hexadecimal code. Sections can then be copied to another disk.

Mechanical and electronic repairs should be left to the specialist. Many businesses specialize in this type of data recovery. An electronic circuit board controller mounted on the drive could fail. It can be replaced, but it takes a skilled electronics technician. The circuit conductors are very fragile and easily broken. Also, disk drive platters can be removed and installed on other drives. However, it takes special tools, training, and a clean room (which is not just a room that is clean). A ***clean room*** is a room where dust and foreign particles have been completely eliminated.

clean room
a room where dust and foreign particles have been completely eliminated.

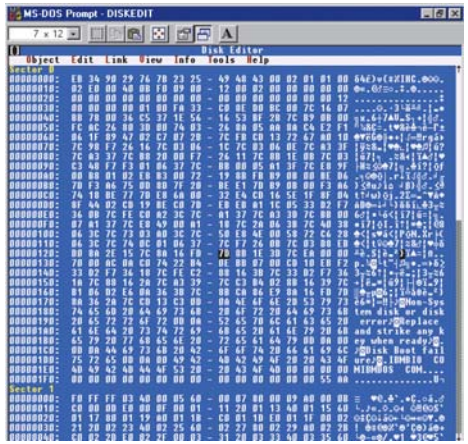


Figure 15-29. Data on a hard drive that stops working can often be accessed using special software. Here a file is being viewed in Norton's Disk Editor.

Preparation for Installing or Upgrading an Operating System

Before installing a new operating system, several appropriate practices should be followed for the ideal setup:

- ✔ Check for viruses.
- ✔ Defrag the drive.
- ✔ Read the readme.txt file.
- ✔ Check the operating system's Web site for latest updates, known installation problems, hardware compatibility lists, patches, and updates.

If you are upgrading an existing system, be sure to backup existing system data. You are probably tired of hearing "back up the system data," but it is the *only way* to rebuild a destroyed system. There are two commonly accepted methods of backing up files: *incremental* and *differential*.

The difference between the two is determined by the *archive bit*. The archive bit is designed to indicate if a file has been backed up or not. This issue is important on large data systems where backups are performed daily to ensure against data loss.

An ***incremental backup*** requires a disk or tape for each daily backup. When performing an incremental backup, only the changes in data since the last incremental or last full backup are copied. A copy of the last full data backup plus *each* incremental backup in sequence must be used to reconstruct an entire collection of data, **Figure 15-30.** When performing a ***differential backup,*** *all* the data changes are copied since the last full backup. Only one disk or tape is needed to perform the differential backup because it copies all changes in data since the last full backup was performed. To restore the data, you need only the last full backup and the last differential backup.

incremental backup operation that backs up select files that have changed since the last backup of files. The archive bit is reset.

differential backup operation that saves files that have changed since the last full backup of all files. The archive bit is not reset.

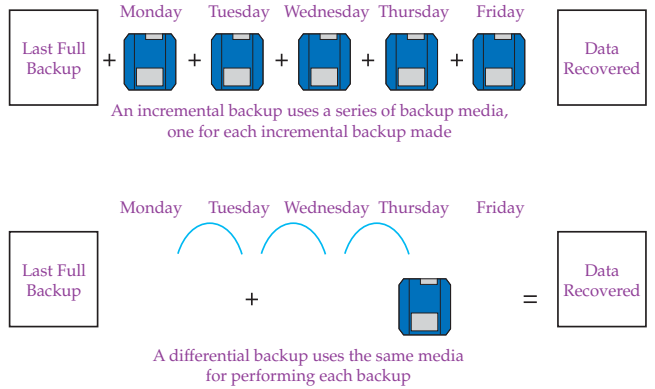


Figure 15-30. The incremental method requires the complete set of disks plus the last full backup to restore the system data. The differential method requires only the last differential backup made plus the last full backup to restore the system.

The reason for selecting an incremental or differential backup is based on the amount of time and disk space required for each type of backup. Since the incremental backup only copies changes from the last incremental backup, there is less data to copy. This results in a shorter time period required to perform the backup. A differential backup copies all data changes since the last full backup. This can require a significant amount of space and time if there is a great number of days between full backups. These differences may seem insignificant at first, but when you are talking about the large volumes of data that some corporations generate, you can be talking about significant periods of time.

Preventive Maintenance

Performing routine maintenance on the PC can help prevent future problems and improve system performance. Some of the most common but often overlooked routine maintenance items are listed in this section. Many of the items can be scheduled to perform automatically.

System Backups

Backups should be performed as part of routine system maintenance. You may not be able to repair a failed computer system, but you can at least restore critical data after installing a clean copy of the operating system. If the system has been configured to perform automatic backups, check if the backups are being performed. The automatic backup configuration may have been turned off or has been corrupted. You can verify that the backup job has run at the scheduled time and that the backup was successful by checking the backup log. Most backup programs keep a backup log, which is accessible through the program's main menu. You should occasionally verify that the data could be read and restored from the backup tape. If you have installed a patch, however, you should verify that you could still restore data. Microsoft has many problems with

their DLL files. A DLL file used in the restore process could develop a problem after a system patch is installed.

Disk Cleanup Utility

The Disk Cleanup Utility can be used to regain hard drive space such as that consumed by temporary files, files sitting in the Recycle Bin, unused Windows components, unneeded installed programs, and restore points created by the System Restore utility. Some of the temporary files that Disk Cleanup allows you to remove are downloaded program files, temporary Internet files, and offline files. The Disk Cleanup Utility performs the functions of other Windows programs, such as Recycle Bin and Add or Remove Programs. From this one utility the Recycle Bin can be emptied, saving you the extra steps of accessing Recycle Bin and clicking Empty Recycle Bin. Windows components and installed programs can be uninstalled, rather than accessing Add or Remove Programs. The Disk Cleanup Utility can be used to remove all but the most recent restore points created by the System Restore utility. System Restore automatically backs up system information. This information can be used to restore a computer to a previously operational state. Depending on factors such as how much hard drive space is available, how much hard drive space is allocated to System Restore, and the amount of activity on the hard drive, System Restore can save one to three weeks of system information in files called *restore points*.

Disk Defragmenter Utility

As you recall from Chapter 9—Magnetic Storage Devices, files can become fragmented over time by opening, closing, and deleting them and by changing their contents. These activities can result in a file being segmented and stored in various clusters across the hard drive. The Disk Defragmenter utility rearranges all files on your hard drive into a continuous series of clusters. This results in better disk performance. The Disk Defragmenter utility should be run at least once per month depending on the amount of file activity on the system, and especially run after using the Disk Cleanup Utility. Also, be aware that running Disk Defragmenter on a large disk, 80 GB or more, can take a very long time. Schedule to run the Disk Defragmenter when you will not require the use of the computer for an extended period of time.

ScanDisk and Chkdsk

Disk error checking should be performed on a regular basis. Windows 98 and Me use the ScanDisk utility, and Windows NT, 2000, XP, and Vista use the Chkdsk utility. Both programs inspect the hard disk and correct errors in the file structure, such as bad sectors, lost clusters, cross-linked files, and directory errors.

Install Patches

Check for the latest software patches for your operating system. Patches should be installed on a regular basis, especially as a matter of security. Many operating system security problems are discovered after the release of an operating system. Checking for and installing patches on a regular basis will keep the security level high on the computer system. Some patches can have adverse effects on your computer system. Be sure to back up your system files before installing a patch.

Virus Protection Updates

Virus protection software requires updates on a regular basis. Your virus protection can fail to protect your system if it does contain the latest virus definitions. Check the company Web site of your virus protection software for the latest virus information and updates.

Clean the Physical System

Routinely check and clean the cooling system on the computer. The cooling system includes the power supply fan(s) and the fans located on critical components such as the CPU, chipset, memory modules, and video cards. Also, remove dust accumulations from passive heat sinks located in the same areas. Dust should be removed using a static-free vacuum cleaner.

Also, be sure to remove dust and debris from keyboards, mouse, and the screen areas. Do not use chemicals when cleaning the plastic parts of a computer system or the screen area. First attempt to clean the plastic parts with a dry, soft, lint-free cloth. Next, try a damp cloth, and as a last resort, you may use a mild, cleaning solution. Keep water away from electronic components inside the computer and computer vents. Avoid the use of any harsh chemicals for cleaning the computer and computer components.

Two Microsoft Web sites provide extensive information that will be very valuable when troubleshooting computers. The first site, http://support.microsoft.com, is designed for the average computer user, and the second Web site, http://technet.microsoft.com, is designed for advanced technicians or IT professionals. Save both links in your Internet Browser because you will most likely be using them often to assist you with computer problems.

Summary

- ✔ Try the simple things first when troubleshooting.
- ✔ Write down changes made as you progress through the troubleshooting stages.
- ✔ A failure during the POST is hardware-related.
- ✔ The PC-Doctor POST card can be used to detect and analyze system failures during the POST.
- ✔ A failure during the loading of the required operating system files and hardware initialization is usually a sign that there is a corrupt system operating file or hardware driver file.
- ✔ A failure after logon is usually a software application or service problem.
- ✔ Hard drives have a high failure rate because mechanical systems have a higher failure rate than electronic systems.
- ✔ You can start the Windows operating system in several different modes, accessed by pressing [F8] when the Windows logo appears.
- ✔ Safe mode loads the minimum generic drivers and bypasses autoexec.bat and config.sys, if they exist.
- ✔ The System Configuration Utility (msconfig.exe) allows users to modify the system configuration.

- ✔ The System Information (msinfo32.exe) utility provides information about the system, as well as online help and access to system troubleshooting tools.
- ✔ Dr. Watson is used to collect information about the computer system before and during a software failure.
- ✔ The DirectX Diagnostic Tool checks the validity of any existing DirectX software tools and add-ons.
- ✔ The System File Checker (sfc.exe) checks for missing, changed, or corrupt system files.
- ✔ Windows XP and Windows 2000 ntdetect.com is now merged into the Windows Vista kernel.
- ✔ The two methods of backing up files are incremental and differential.
- ✔ Performing regularly scheduled maintenance can prevent future problems and improve system performance.

Review Questions

Answer the following questions on a separate sheet of paper. Please do not write in this book.

1. What are the three major fault areas?
2. What is *most likely* the cause of a failure during POST?
3. How can you tell that the system kernel has been loaded in the Windows operating system?
4. If there are no power lights and the fan is not running, which is *most likely* the cause?
   a. Power supply
   b. Motherboard
   c. Hard drive
   d. CMOS settings
5. You can start the PC in safe mode after pressing _____.
   a. [Ctrl] [Alt] [Del]
   b. [F8]
   c. [F3]
   d. [Ctrl] [Shift] [Del]
6. How does safe mode differ from a normal boot process?
7. How can you access the **Advanced Boot Options** menu in Windows Vista?
8. What troubleshooting utility is available in Windows XP that can be used when you cannot access the GUI interface or safe mode?
9. How do you start the Windows Recovery Environment in Windows Vista?
10. What are the five Windows Recovery Environment options in Windows Vista?
11. What is the Windows XP ASR utility?
12. What utility can be used to eliminate services and applications while troubleshooting a computer problem?
13. What program allows you to directly access the registry files?
14. Which four hardware resources are monitored by the Reliability and Performance utility?

15. What boot sequence step is similar to all Windows operating systems?
16. How can you change the drive search order from drive C to the DVD drive as the first drive looked at for booting purposes?
17. What is used in place of the win.ini and system.ini files to store system information?
18. What does the ntldr file do?
19. What is the gdi.exe used for in the Windows 2000 and XP operating system?
20. What is the name of the Windows 2000 and XP kernel file?
21. What is the final step to the boot process in a Windows 2000 and XP installation?
22. What are some things you should do before installing a new operating system?
23. List seven things to perform during regular system maintenance.
24. What is the difference between an incremental backup and a differential backup?

Sample A+ Exam Questions

Answer the following questions on a separate sheet of paper. Please do not write in this book.

1. How do you access safe mode in Windows XP while the system is booting?
   a. Press the [Del] key.
   b. Press the [F8] key.
   c. Press [Ctrl] [Alt] [Del].
   d. Hold down the Windows logo key.
2. Which of the following typically causes a failure during the POST?
   a. Corrupt operating system boot files.
   b. A printer driver.
   c. A critical hardware device.
   d. A software application.
3. Which two files are required to load the Windows XP operating system? (Select two.)
   a. ntldr
   b. ntoskrnl.exe
   c. autoexec.bat
   d. cmd.com
4. What is the name of the Windows XP kernel?
   a. ntldr
   b. ntoskrnl.exe
   c. ntdetect.com
   d. service.exe
5. What key combination is used to access the Windows XP logon dialog box?
   a. [Ctrl] [Esc] [Alt]
   b. [Ctrl] [Alt] [Del]
   c. [Ctrl] [Shift] [Tab]
   d. [Ctrl] [Shift] [Esc]

6. Which is the recommended way to back up the system registry files in Windows XP?
   a. Insert the Windows XP installation CD into the CD drive. Reboot the computer and then select **Backup registry** from the menu.
   b. The Windows XP registry is backed up each time the operating system is started.
   c. Open **Control Panel** and then double-click the **Registry Backup and Restore** icon.
   d. Create a restore point.
7. How do you access the System Restore feature in Windows XP?
   a. **Start | All Programs | System Restore.**
   b. **Start | All Programs | Accessories | System Tools | System Restore.**
   c. Right-click **My Computer**, select **Properties** from the shortcut menu, and then select the **System Restore** tab.
   d. **Start | All Programs | Accessibility | System Restore.**
8. What command can be run to view and manually edit the system registry in Windows XP?
   a. **msconfig**
   b. **sysconfig**
   c. **boot.ini**
   d. **regedt32**
9. What command can be issued to view the Windows XP System Configuration Utility?
   a. **sfc**
   b. **sysconfig**
   c. **msconfig**
   d. **regedit**
10. What would be used to diagnose a problem that occurs during the POST phase of the system boot operation?
    a. A POST card.
    b. A multimeter.
    c. Windows System Configuration Utility.
    d. A DOS disk.

Suggested Laboratory Activities

Do not attempt any suggested laboratory activities without your instructor's permission. Certain activities can render the PC operating system inoperable.

1. Launch **msinfo32.exe** from **Start | Run** in Windows XP or **Start | Search** in Windows Vista. View all the information related to the system.
2. Launch **msconfig.exe** from the **Start | Run** in Windows XP or **Start | Search** in Windows Vista. Look at all the options available that can be used to diagnose a system problem. Try stopping the loading of a specific software application and observe the results.
3. Access the boot options menu in both Windows XP and Windows Vista. Press the [F8] key during the boot to access the menu, and then select **Safe mode** option to observe the effect on the operating system. See what files and programs can be accessed and run during safe mode.

4. Using a specific workstation designated for experimentation by your instructor, try several of the following tests:
   - ✔ Remove the data cable from the hard disk drive and boot the system to observe any error messages.
   - ✔ Perform a complete PC backup using Windows Vista. The backup utility is located at **Start | All Programs | Maintenance | Backup and Restore Center**.
   - ✔ Run **regedt32** in Windows XP and Windows Vista and inspect the contents of the registry. Do not make any changes to any of the contents.
   - ✔ Open the **Problem Reports and Solutions** in Windows Vista located at **Start | All Programs | Maintenance | Problem Reports and Solutions**. After opening the utility, explore the features available, but be careful not to select the **Clear solution and problem history** option.
5. Visit the Microsoft TechNet Web site and look at all the available features for technicians.
6. Visit the following Web sites and look at the information about BIOS beep codes:
   - ✔ www.ami.com
   - ✔ www.phoenix.com
   - ✔ http://bioscentral.com
7. Visit the Dell Advanced Troubleshooting Web page at http://support.dell.com/support/edocs/systems/dim2300C/advanced.htm and look at the information provided to assist with troubleshooting Dell Computers.
8. Run the Windows Vista Memory Diagnostics Tool (mdsched.exe) from the command prompt.

Interesting Web Sites for More Information

http://bioscentral.com

http://support.dell.com/support/edocs/systems/dim2300C/advanced.htm

http://support.microsoft.com

www.ami.com

www.bioscentral.com/postcodes/awardbios.htm

www.computerhope.com/beep.htm

www.configsafe.com

www.pc-doctor.com

www.phoenix.com

www.sysinternals.com

www.winternals.com

Chapter 15
Laboratory Activity
Advanced Boot Options

After completing this laboratory activity, you will be able to:

- ✔ Access the **Advanced Boot Options** menu.
- ✔ Explain the purpose of each **Advanced Boot Options** menu option.
- ✔ Explain the purpose of the ntbtlog.txt file.
- ✔ Explain why the **Advanced Boot Options** menu may not be available to a technician.

Introduction

One of the most important steps in troubleshooting a PC system is accessing the Windows **Advanced Boot Options** menu. This menu is accessible only after a successful POST has been completed. If you cannot access the **Advanced Boot Options** menu, you most likely have a hardware problem and the computer did not successfully complete POST. Another reason you will not be able to access the **Advanced Boot Options** menu is because required system startup files are corrupted. If system files are corrupted, you will need to reinstall the system files.

The most common option in the **Advanced Boot Options** menu is **Safe mode**. This option allows the computer to finish the complete boot sequence, but with a minimal number of drivers and services. Drivers and services are often the cause of a computer system failing to complete the boot process. By loading only a minimal number of drivers and services, a failed computer system can be often started and repaired while in safe mode.

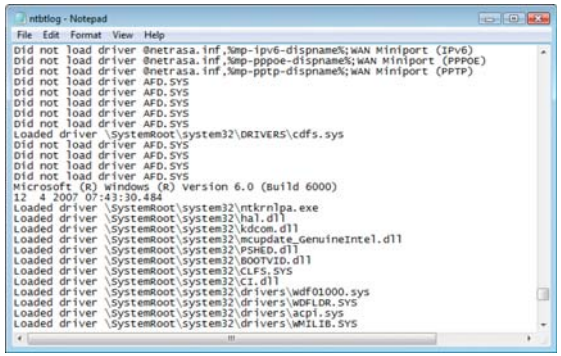
The **Advanced Boot Options** menu is accessed at startup by pressing the [F8] key after POST and before loading the operating system. The following table describes each menu option. Similar options are available in Windows XP.

Advanced Boot Option	Description
Safe Mode	Starts the operating system with only the minimal drivers and services required to operate the system.
Safe Mode with Networking	Includes the necessary network adapter drivers and services needed to establish a network connection.
Safe Mode with Command Prompt	Starts with the command prompt rather than the GUI. Requires fewer drivers this way.
Enable Boot Logging	Creates a log file called ntbtlog.txt, which lists all the drivers installed during the startup sequence.
Enable Low-Resolution Video (640x480)	Uses the lowest possible video resolution and a low refresh rate for minimal impact of system resources.
Last Known Good Configuration (advanced)	Starts Windows using the last set of successful registry and configuration settings.
Directory Services Restore Mode	Used for starting a domain controller for directory support.
Debugging Mode	Used for advanced troubleshooting, usually by programmers. Sends information to another computer via a serial connection.
Disable Automatic Restart on System Failure	Will not let the system automatically restart on a boot failure.
Disable Driver Signature Enforcement	Does not require drivers to have a driver signature.
Start Windows Normally	Starts Windows normally, not with any reduced drivers, services, or configuration.

As a computer repair technician, your main interest will be the following four boot options: **Safe Mode**, **Safe Mode with Networking**, **Safe Mode with Command Prompt**, and **Last Known Good Configuration**.

Safe Mode is the most commonly accessed option when troubleshooting a computer using the **Advanced Boot Options** menu. It loads only the bare minimum drivers required to run the system. Once the computer is started in safe mode, you can access other utilities such as System Restore, System Configuration Utility, Backup, other troubleshooting tools.

By selecting the **Enable Boot Logging** option, the ntbtlog.txt will be created during the system boot. The ntbtlog.txt file contains a list of all drivers loaded and not loaded during the boot. This information can help you determine what driver file the computer is having problems loading. The ntbtlog.txt file can be read using Notepad or a similar software application. The following screen capture shows an example of the ntbtlog.txt file contents. As you can see, all drivers are clearly identified as either "Loaded driver" or as "Did not load driver."


ntbtlog - Notepad
File Edit Format View Help
Did not load driver @netrasa.inf,%mp-ipv6-dispname%;WAN Miniport (IPv6)
Did not load driver @netrasa.inf,%mp-pppoe-dispname%;WAN Miniport (PPPOE)
Did not load driver @netrasa.inf,%mp-pptp-dispname%;WAN Miniport (PPTP)
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Loaded driver \SystemRoot\system32\DRIVERS\cdfs.sys
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Did not load driver AFD.SYS
Microsoft (R) Windows (R) Version 6.0 (Build 6000)
12 4 2007 07:43:30.484
Loaded driver \SystemRoot\system32\ntkrnlpa.exe
Loaded driver \SystemRoot\system32\hal.dll
Loaded driver \SystemRoot\system32\kdcom.dll
Loaded driver \SystemRoot\system32\mcupdate_GenuineIntel.dll
Loaded driver \SystemRoot\system32\PSHED.dll
Loaded driver \SystemRoot\system32\BOOTVID.dll
Loaded driver \SystemRoot\system32\CLFS.SYS
Loaded driver \SystemRoot\system32\CI.dll
Loaded driver \SystemRoot\system32\drivers\Wdf01000.sys
Loaded driver \SystemRoot\system32\drivers\WDFLDR.SYS
Loaded driver \SystemRoot\system32\drivers\acpi.sys
Loaded driver \SystemRoot\system32\drivers\WMILIB.SYS

The computer will automatically start up in a modified boot menu called **Windows Error Recovery** if the computer did not shut down properly—for example, if you shut the computer down with the power switch rather than use the option from the **Start** menu. There will be only four choices to choose from: **Safe Mode**, **Safe Mode with Networking**, **Safe mode with Command Prompt**, **Start Windows Normally**. If no selection is made in approximately 30 seconds, the computer will automatically select the **Start Windows Normally** option.

Equipment and Materials

✔ PC with the Windows Vista operating system installed. (You may substitute a Windows XP system for this lab activity.)

Procedure

1. _____ Boot the computer and wait for the desktop to be displayed. This step is to ensure your system is working properly.
2. _____ Restart the PC and press [F8] during the boot sequence to access the **Advanced Boot Options** menu. At times, it is very difficult to catch the exact moment when POST ends and the loading of the operating system begins. You can try tapping the [F8] key repeatedly after the computer starts and continue until the **Advanced Boot Options** menu appears on the screen. If you cannot access the **Advanced Boot Options** menu, call your instructor for assistance.
3. _____ After the **Advanced Boot Options** menu appears, select the **Safe Mode** option.
4. _____ When the computer starts in safe mode, the words "Safe Mode" will appear in all four corners of the display. The desktop background will be black. Also, the screen resolution is reduced.
5. _____ On a separate sheet of paper, make a list of all **Advanced Boot Options** menu options.

6. _____ Copy the following list of items on a separate sheet of paper and indicate if each can be accessed during safe mode operation. Indicate each item with a "yes" or "no."
   Backup and Restore _____
   Windows Remote Assistance _____
   Command Prompt _____
   System Tools _____
   System Restore _____
   Access the Internet _____
   Event Viewer _____
   Task Manager _____
   Control Panel _____
7. _____ Now, reboot the computer and let the computer start normally. Do not press the [F8] key.
8. _____ Shut down the computer using the power on-off button. Restart the computer and see which boot options are available to you. List the available options on a separate piece of paper.
9. _____ Now, reboot the computer and select **Safe Mode with Command Prompt** from the **Advanced Boot Options** menu. Answer the following question on a separate piece of paper.
   Is the user interface text mode only or graphic user interface?
10. _____ Type and enter the **dir** command at the command prompt and observe the action.

Note:
To stop the directory command, press [Ctrl] [Pause Break].

11. _____ Type and enter **exit** at the command prompt. Then, press [Ctrl] [Alt] [Del] and click the **Shut down** button in the lower-right corner of the display. This will shut down the computer.
12. _____ Restart the computer and then use [F8] to open the **Advanced Boot Options** menu.
13. _____ Select the **Enable Boot Logging** option to create a driver status log.
14. _____ Look in the root directory and look under the Windows folder to see if the ntbtlog.txt file exists. The file is a hidden system file, so you will need to change the folder options to show hidden files. You can do this by opening an Explorer window and selecting **Tools | Folder Options | Show hidden files and folders**. You can use the **Start** menu **Search** box to assist you in locating the file. After the file is opened, look at its contents. Close the file and shut down the computer.
15. _____ Now, restart the computer and select **Safe Mode** from the **Advanced Boot Options** menu.
16. _____ After the computer enters safe mode, type **msconfig** into the **Search** box to start the System Configuration Utility. After the **System Configuration Utility** dialog box opens, select the **Services** tab to observe which services were loaded. All services should be marked "Stopped" under the "Status" column.
17. _____ Close the System Configuration Utility and then shut down the computer.

18. _____ You may spend a few minutes exploring the **Advanced Boot Options** menu at this time. If you are having difficulty opening the **Advanced Boot Options** menu, take some time to practice.
19. _____ Return the workstation to its original condition and then go on to answer the review questions.

Review Questions

Answer the following questions on a separate sheet of paper. Please do not write in this book.

1. Which function key is used to access the **Advanced Boot Options** menu?
2. Which options are available when restarting a computer after turning off the computer using the power switch?
3. Can you access Control Panel while in safe mode?
4. Can you run **msconfig** from the **Search** box while in safe mode?
5. What is contained in the ntbtlog.txt file?
6. Where is the ntbtlog.txt file located?
7. Can you run the System Configuration Utility while in safe mode?
8. What services are shown running in the System Configuration Utility during safe mode?
9. What words appear in the four corners of the display during safe mode?
10. What would cause the **Advanced Boot Options** menu or safe mode not to be available?

Disassembly of an older (or nonfunctioning) hard drive will allow you to see how the mechanical and electronic parts of a hard drive work together. Do not attempt to open any hard drive that you intend to use again for data storage. Once a hard drive case has been opened, the drive cannot be used.